NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

ADOPTING CLOUD COMPUTING IN THE PAKISTAN NAVY

by

Tahir Majeed Asim

June 2015

Thesis Advisor: Dan Boger
Co-Advisor: Dorothy E. Denning

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE

Form Approved OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	**2. REPORT DATE** June 2015	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
ADOPTING CLOUD COMPUTING INTHE PAKISTAN NAVY

5. FUNDING NUMBERS

6. AUTHOR(S) Tahir Majeed Asim

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES)
N/A

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT (maximum 200 words)

Pakistan's proximity to the Strait of Hormuz, through which millions of barrels of oil is shipped per day, makes it a gateway to Central Asian countries. The Pakistan coastline stretches to almost 1,000 kilometers and has an exclusive economic zone of 290,000 km^2. As a flag bearer of protecting the country's sea lines of communication and safeguarding its maritime territories, the Pakistan Navy is in the continuous process of modernization. Although a robust command and control structure exists for the accomplishment of peacetime and wartime objectives, there is still a need to adopt up-to-date procedures that can ensure the two-way exchange of information in near real-time and provide access to information from anywhere around the globe.

This thesis explores the peculiarities of cloud computing and its potential utility to the Pakistan Navy. After an in-depth analysis of the country's information technology environment, the scope and utility of cloud computing in the country, and the U.S. Department of Defense, the U.S. Navy, and the National Institute of Standards and Technology cloud architectures, a framework has been laid out for adopting cloud computing in the Pakistan Navy.

14. SUBJECT TERMS
Cloud computing, IT industry in Pakistan, US Navy cloud, NIST cloud architecture, DoD cloud

15. NUMBER OF PAGES
83

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	**18. SECURITY CLASSIFICATION OF THIS PAGE**	**19. SECURITY CLASSIFICATION OF ABSTRACT**	**20. LIMITATION OF ABSTRACT**
Unclassified	Unclassified	Unclassified	UU

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

ADOPTING CLOUD COMPUTING IN THE PAKISTAN NAVY

Tahir Majeed Asim
Lieutenant Commander, Pakistan Navy
B.E., National University of Sciences and Technology, 2004

Submitted in partial fulfillment of the
requirements for the degree of

**MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(COMMAND, CONTROL & COMMUNICATIONS)**

AND

MASTER OF SCIENCE IN INFORMATION OPERATIONS

from the

**NAVAL POSTGRADUATE SCHOOL
June 2015**

Author: Tahir Majeed Asim

Approved by: Dr. Dan Boger
Thesis Advisor
Chair, Department of Information Sciences

Dr. Dorothy E. Denning
Co-Advisor

Dr. John Arquilla
Chair, Department of Defense Analysis

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

Pakistan's proximity to the Strait of Hormuz, through which millions of barrels of oil is shipped per day, makes it a gateway to Central Asian countries. The Pakistan coastline stretches to almost 1,000 kilometers and has an exclusive economic zone of 290,000 km^2. As a flag bearer of protecting the country's sea lines of communication and safeguarding its maritime territories, the Pakistan Navy is in the continuous process of modernization. Although a robust command and control structure exists for the accomplishment of peacetime and wartime objectives, there is still a need to adopt up-to-date procedures that can ensure the two-way exchange of information in near real-time and provide access to information from anywhere around the globe.

This thesis explores the peculiarities of cloud computing and its potential utility to the Pakistan Navy. After an in-depth analysis of the country's information technology environment, the scope and utility of cloud computing in the country, and the U.S. Department of Defense, the U.S. Navy, and the National Institute of Standards and Technology cloud architectures, a framework has been laid out for adopting cloud computing in the Pakistan Navy.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

LIST OF FIGURES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ANSI	American National Standards Institute
AWS	Amazon web services
CIA	Confidentiality Integrity Availability
CIO	Chief information officer
CMF	Combined Maritime Forces
CSP	Cloud service provider
CWCS	Cube XS Weatherly cloud services
DISA	Defense Information Systems Agency
DOD	Department of Defense
DON	Department of Navy
DoS	Denial of service
IaaS	infrastructure as a service
IA	Information assurance
ISP	Internet service provider
IT	Information technology
JIE	Joint information environment
NATO	North Atlantic Treaty Organization
NIPRNet	Nonsecure IP router network
NIST	National Institute of Standards and Technology
PaaS	Platform as a service
PTCL	Pakistan telecommunication limited
SaaS	Software as a service
SAN	storage area network
SIPRNet	Secure IP router network
SLA	Service level agreement
TCP	Transmission control protocol
TIA	Telephone industry association
VLAN	Virtual local area network
VPN	Virtual private network
WiMAX	Worldwide interoperability for Microwave access

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

> Read! In the name of your Lord who created—Created the human from something which clings. Read! And your Lord is Most Bountiful—He who taught (the use of) the Pen, Taught the human that which he knew not.
>
> —First revealed verses of Qur'an, Al-Alaq 96:1-5

I bow my head and thank Almighty Allah for giving me the opportunity to seek a Master's degree at the Naval Postgraduate School and for providing me with the strength, wisdom, and perseverance to complete both my master's programs simultaneously.

I am extremely indebted to the faculty of the Information Sciences and Defense Analysis Department at the Naval Postgraduate School for their continuous guidance, support, and professionalism. I am particularly thankful to Dr. Dan Boger and Dr. Dorothy E. Denning for their supervision and complete insight on the topic. Their experience in cloud computing was a great help for me to focus my thoughts and complete this research. I would like to express my gratitude to my colleagues at Naval Postgraduate School, who provided the ideal atmosphere to make this learning a worthwhile experience.

Finally, I am extremely grateful to my beloved father, who passed away during my stay at Naval Postgraduate School; my beloved mother; my brothers and sisters; my lovely wife, Adeela; and my adorable son Hishaam, for their prayers, affection, and patience, without which this modest endeavor would not have been possible.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

> I don’t need a hard disk in my computer if I can get to the server faster. … Carrying around these non-connected computers is byzantine by comparison.
>
> Steve Jobs (Speech, 1997)

In the course of recent decades, the world has encountered an upset in information technology (IT), and various new techniques for the rapid exchange of information have evolved. This evolution is all about the exchange of information in real time from anywhere around the globe and using this information to perform a variety of tasks. This evolutionary technology known as cloud computing has been adopted worldwide by industries, businesses, educational institutes, government organizations, defense institutes, and armed forces.

Given the current growth rate of the cloud computing industry, it is predicted that by year 2020, its global market will reach $270 billion (Market Research, 2014). This makes cloud computing among the leading revenue-generating and rapidly growing industries in the world. Cloud computing is offering better insight and visibility for analysis, better collaboration, easy access to information, and availability of enormous storage and computing resources at affordable cost. Cloud computing is being adopted globally to meet the challenges of the corporate world and to handle the rapidly growing needs of computation and analytical tools. Cloud computing has enhanced users' capacity to use framework and assets innovatively, and it can be used in a variety of ways to meet individual needs. Cloud computing is available to users in four forms: private cloud, hybrid cloud, community cloud, and public cloud. The form of the cloud to be chosen depends primarily on the data classification, the data type, business or organization needs, and the methodology for accessing the data.

Many developed countries such as Japan, the United States, China, Russia, and France have been exploiting the benefits of cloud computing for over a decade. Likewise, the military forces of many countries have also adopted cloud computing as an integral component of military operations conducted either locally or remotely. With the use of

cloud services, military forces are able to remotely access data from data centers located thousands of miles away from the theater of operations. Data can be retrieved by all services of the military and eventually help in building a clear, concise, error-free, homogenous, unambiguous, and up-to-date picture for military commanders. Furthermore, cloud computing can be used by multiple services to conduct coordinated joint operations.

Cloud computing provides all essential information to military commanders that is considered very important for successful conduct of operations and help in decision-making. In the aftermath of the 9/11 attacks and following the U.S. invasions of Iraq and Afghanistan, Pakistan joined the Global War on Terror. Since then, Pakistan has become a major non-NATO ally of the United States and has demonstrated its will and strength to curb the menace of terrorism. So far, Pakistan has suffered more than 60,000 casualties in numerous terrorist attacks and bombings across the country, and among these, more than 6,000 casualties were from the military forces. The Pakistan Navy, which is a medium to smaller size force, is fighting this war on multiple fronts. Besides conducting several successful coalition patrols in the Indian Ocean, the Navy has also successfully foiled a number of attempts at human trafficking, arms smuggling, and piracy. In addition, the Pakistan Navy is participating in various multinational exercises and hosting exercises of similar scope at home. However, in the absence of a Pakistan Navy cloud, a vacuum exists with limited access to data and information resources ashore.

The Pakistan Navy is still in the process of modernization and is upgrading its equipment to conduct counter-piracy and counterterrorism operations more sturdily. In parallel with other developing countries of the region, the Pakistan Navy is also facing the challenge of adopting cloud computing, which will allow for the sharing of resources, better command and control, enhanced situational awareness, and easy access to operational information for quick and better decision-making.

A. THESIS OVERVIEW

This thesis postulates that in today's rapidly advancing IT environment, the use of cloud computing will help the Pakistan Navy to access data remotely from high seas and will ultimately provide better coordination, better sharing of intelligence and surveillance reports, better decision-making, a robust command structure, and a swift means for the exchange of all forms of data among units at sea and with shore authorities. This thesis draws inferences from the U.S. DOD strategy, the U.S. Navy's roadmap, and the National Institute of Standards and Technology (NIST) reference architecture for adopting cloud computing. This thesis focuses on the current IT environment of Pakistan and recommends a framework for adopting cloud computing in the country's navy. The proposed cloud architecture is a generic framework for adopting cloud computing, and shore-based cloud infrastructure will require interface with sea-based cloud infrastructure, which will be more focused on tactical requirements of units afloat.

B. STRUCTURE OF THE STUDY

This thesis is divided into six chapters, including this chapter. Chapter II provides background information on the key concepts, definitions, and various models and categories of cloud computing as well as the benefits and risks associated with cloud computing. Chapter III discusses the scope of cloud computing in Pakistan and the utility of cloud computing in the industrial and corporate sectors of the country. It also provides details about reputed government-owned and privately owned cloud service providers in the country. Chapter IV analyzes the U.S. DOD cloud computing strategy, the U.S. Navy's roadmap to cloud computing, and the NIST reference architectures for cloud computing. This chapter formulates a framework for adoption of cloud computing for the Pakistan Navy. Chapter V focuses on how to implement this recommended framework and on a suitable model for using cloud services. The final chapter endeavors to draw conclusions and recommendations for the Pakistan Navy and to offer suggestions for future research.

THIS PAGE INTENTIONALLY LEFT BLANK

II. CLOUD COMPUTING

The concept of cloud computing is not new, but its usage is more prevalent than ever before. Cloud computing in its various forms enables organizations, enterprises, and firms to remotely access their data from geographically distributed data centers worldwide. Cloud computing is being embraced by different associations to meet the challenges of the corporate world and to handle the rapidly growing needs of computation and analytical tools.

Cloud computing offers a low cost, relatively fast solution to information technology (IT) problems. Cloud computing has enhanced the ability of users to re-provision technological infrastructure and delivering of services. The creation of the Internet marked a milestone in computer utility by creating an overall arrangement of systems that empowers singular computers to communicate with any computer universally (Buyya, Yeo, Venugopal, Broberg & Brandic, 2009). Computational power and storage available through cloud computing allows well-known or specialized software and web applications to execute programs (Gupta, Kumar & Abraham, 2013). Consequently, cloud computing has eased the burden of organizations in running or managing data centers, updating and patching software, and reducing IT expenditures.

Beyond commercial usage, cloud computing is being adopted by modern military forces for remotely accessing data, for sharing information with sister services during coordinated operations, for sharing videos from predators, and for many other applications during a range of scenarios. Many developed countries such as the United States, China, Russia, and France have been exploiting the benefits of various models of cloud computing for over a decade. Data from cloud servers can be retrieved by all service branches of the military and can eventually help in building a clear, concise, error-free, homogenous, unambiguous, and up-to-date picture for military commanders.

A. TERMS RELATED TO CLOUD COMPUTING

Before proceeding further, there are a few terminologies related to cloud computing as defined by National Institute of Standards and Technology:

- **Cloud Consumer**: A person or organization that maintains a business relationship with, and uses service from, cloud provider.
- **Cloud Provider**: A person, organization, or entity responsible for making a service available to interested parties.
- **Cloud Carrier**: An intermediary that provides connectivity and transport of cloud services from cloud providers to cloud consumers.
- **Cloud Auditor**: A party that can conduct independent assessment of cloud services, information system operations, performance, and security of the cloud implementations.
- **Cloud Broker**: An entity that manages the use, performance, and delivery of cloud services and negotiates relationships between Cloud Provider and Cloud Consumer (National Institute of Standards and Technology [NIST], 2011a).

B. WHAT IS CLOUD COMPUTING?

As defined by NIST, cloud computing is "a model for enabling ubiquitous, convenient, and on-demand network access to a shared pool of configurable computing resources that can be rapidly provisioned and released with minimal management effort or service provider interaction" (NIST, 2011b). Figure 1 elaborates this definition and shows how remote users are able to retrieve data, run various applications, and perform a variety of tasks from their portable devices and computers.

Figure 1. Cloud Computing Model

In cloud computing both the paradigm and deployment models are evolving (Plummer et al., 2009). Cloud computing is not intricate; it is simply effective servers that store or run applications and provide a main issue of repetitive communications (Scholz, 2013). Cloud computing is a scalable, efficient, and economical solution for storage and computing, and it is managed by a cloud service provider (CSP; Thampsi, Bhargava, & Atrey, 2013). Cloud computing services do not oblige end-client information of the physical area or setup of the framework that delivers these services (Zhou, 2012). The assets of cloud computing can be contracted on rent, which helps build the asset usage of the IT foundation (Thampsi et al., 2013).

1. Cloud-Based Models

There are four basic models of cloud computing, which can be identified based on ownership of resources and distribution of data.

Private Cloud

Private cloud refers to an IT domain in which assets and services are possessed by the association that uses them (Orakwue, 2010). The private cloud empowers an association to delve into cloud building design without giving up control, corporate administration, or dependability (Krutz & Vines, 2010). The private cloud is an expensive model that involves sharing data over the intranet and limiting the exchange of information outside of it via a secure channel (Geczy, Izumi, & Hasida, 2012). Security, hardware and software needs, and data center management are all handled by the organization itself. This model is perfectly matched to the individual needs of a single organization. Figure 2 below shows all infrastructure and resources required for providing cloud services are under one umbrella of an organization's IT setup.

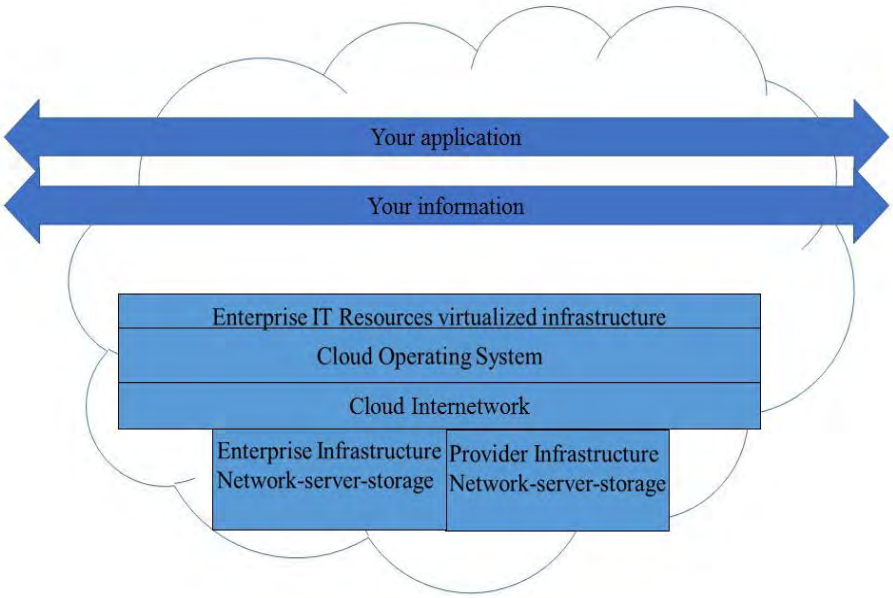


Figure 2. Private Cloud Model

Public Cloud

Public cloud refers to a model in which IT needs are outsourced and the organization does not own its IT resources (Hofmann & Woods, 2010). Due to the outsourcing, IT requirements are not tailored to the individual firm's needs (Geczy et al., 2012). A public cloud is managed at a data center claimed by a cloud services provider that has different customers and uses dynamic provisioning (Krutz & Vines, 2010). This model is open for public use as elaborated in Figure 3 and is most vulnerable to attacks by hackers and to eavesdropping.

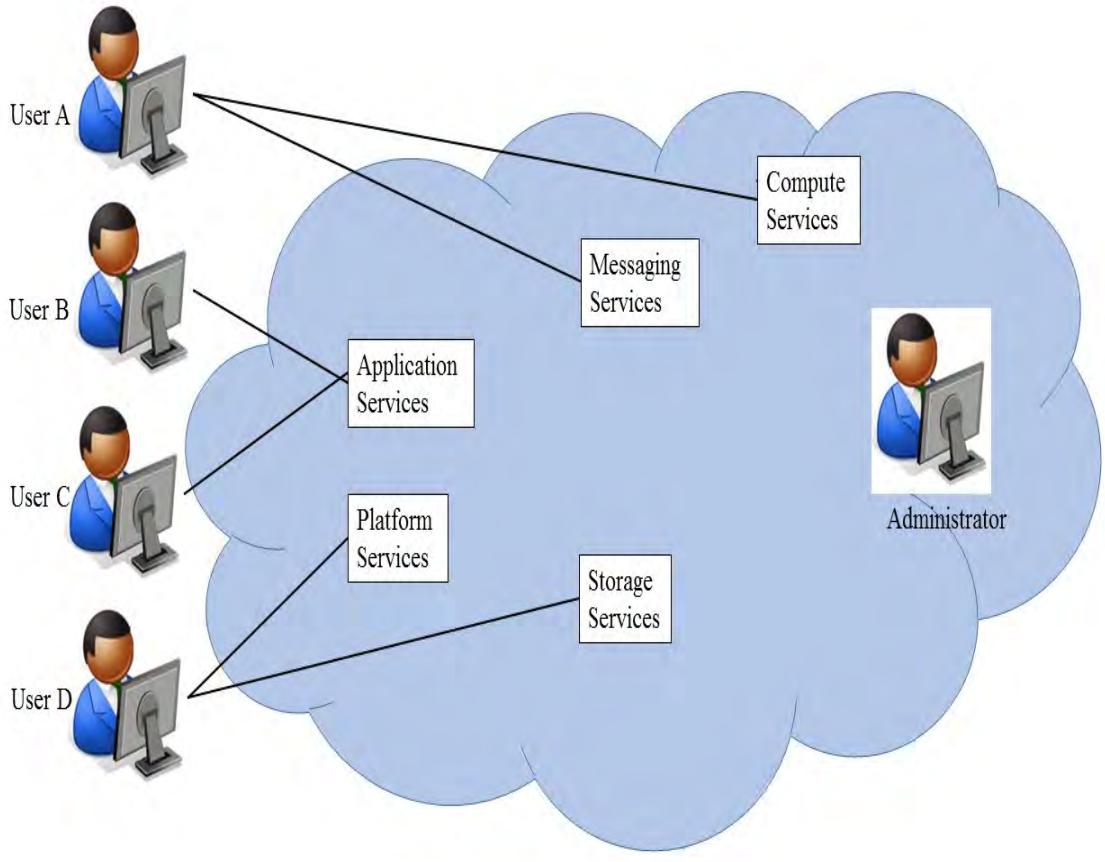


Figure 3. Public Cloud Model

Hybrid Model

A *hybrid model* is used when an organization needs to maintain two different models based on the criticality of its information. The firm possesses its essential IT resources and facilities, while noncritical services are outsourced to external providers (Sotomayor, Montero, Llorente & Foster, 2009). This model may be adopted when an organization wants to roll out a new system on its private cloud; before increasing its private cloud capacity, the new system may be hosted on a public cloud to check the market response (Winkler, 2011).

Community Cloud

As the name implies, *community cloud* describes a mutual framework that is utilized by and upheld by numerous organizations (Krutz & Vines, 2010). The shared cloud asset may be utilized by firms that have overlying contemplations and targets (Krutz & Vines, 2010). Figure 4 indicates that a community cloud may be owned or operated by an organization or business firm or a combination of both.

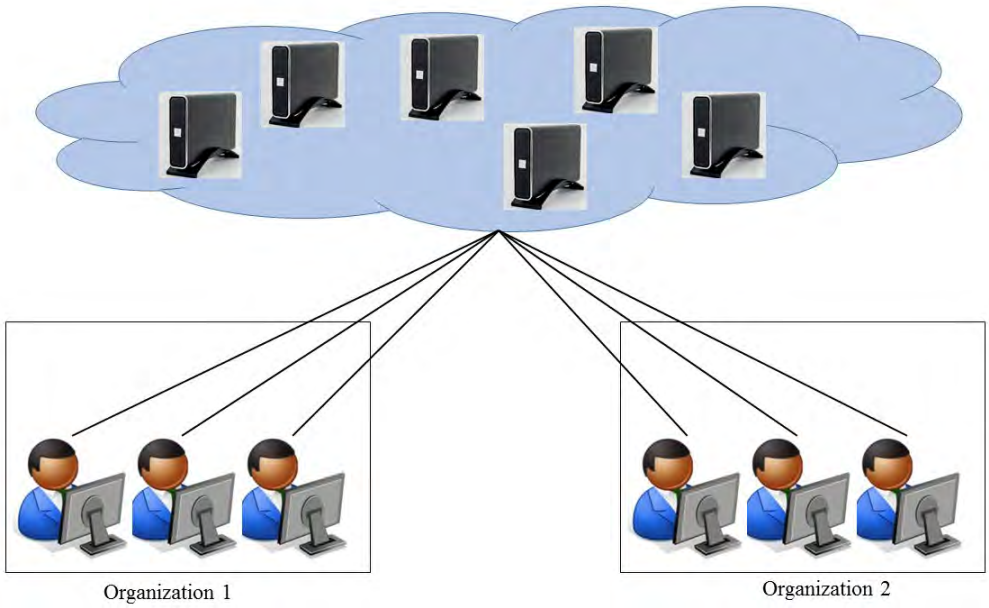


Figure 4. Community Cloud Model

2. Categories of Cloud Services

Cloud computing services can be adopted by an organization in three different forms: infrastructure, software, and hardware.

Infrastructure as a Service

NIST defines *infrastructure as a service* (IaaS) as

> "the capability provided to the consumer to provision processing, storage, networks, and other fundamental computing resources; the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications and may have limited control of select networking components". (NIST, 2011b)

IaaS delivers virtualized resources, such as visitor virtual machines, storage, or database services (Winkler, 2011). In Figure 5, the end user is running the applications over the cloud infrastructure provided by the cloud provider.

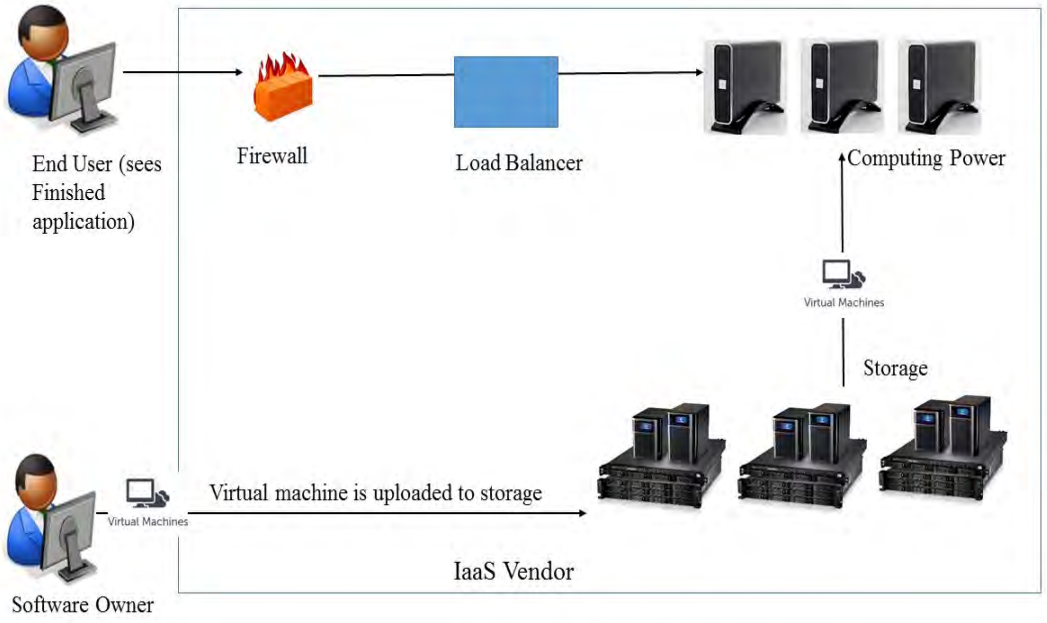


Figure 5. IaaS Model

Software as a Service

Software as a service (SaaS) as defined by NIST is "the capability provided to the consumer to use the provider's applications running on a cloud infrastructure, which are accessible from various client devices through either a thin client interface such as a web browser or a program interface" (NIST, 2011b).

SaaS consumers do not control the basic cloud base, servers and working frameworks, or individual applications. The capital expense of software licensing is saved by renting the software instead of purchasing the software, which is the more traditional method. Thus, in Figure 6, cloud users are using software stored on a web server via the Internet.

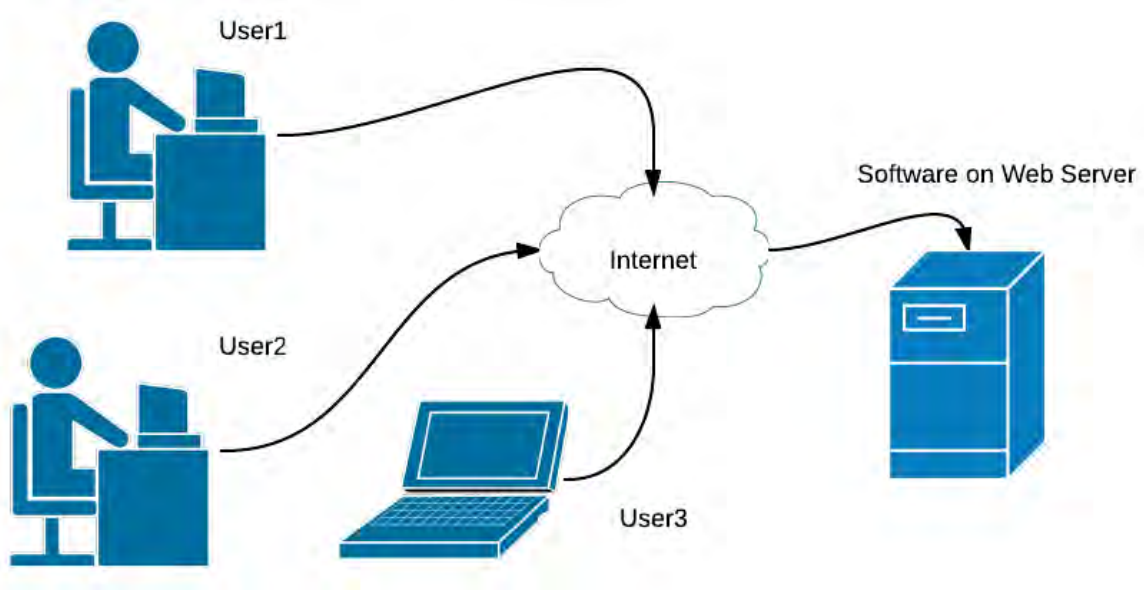


Figure 6. SaaS Model (from WebDweb Web Systems, n.d.)

Platform as a Service

In platform as a service (PaaS), the user hosts and controls an environment for its applications but does not control the working framework, equipment, or system foundation (Antonopoulos & Gillam, 2010). PaaS providers convey a packaging of programming and framework and give a cloud to an end client to host their own particular created applications or services (Winkler, 2011). In Figure 7 below, business users are using applications specific to their business on cloud services developed by the cloud provider.

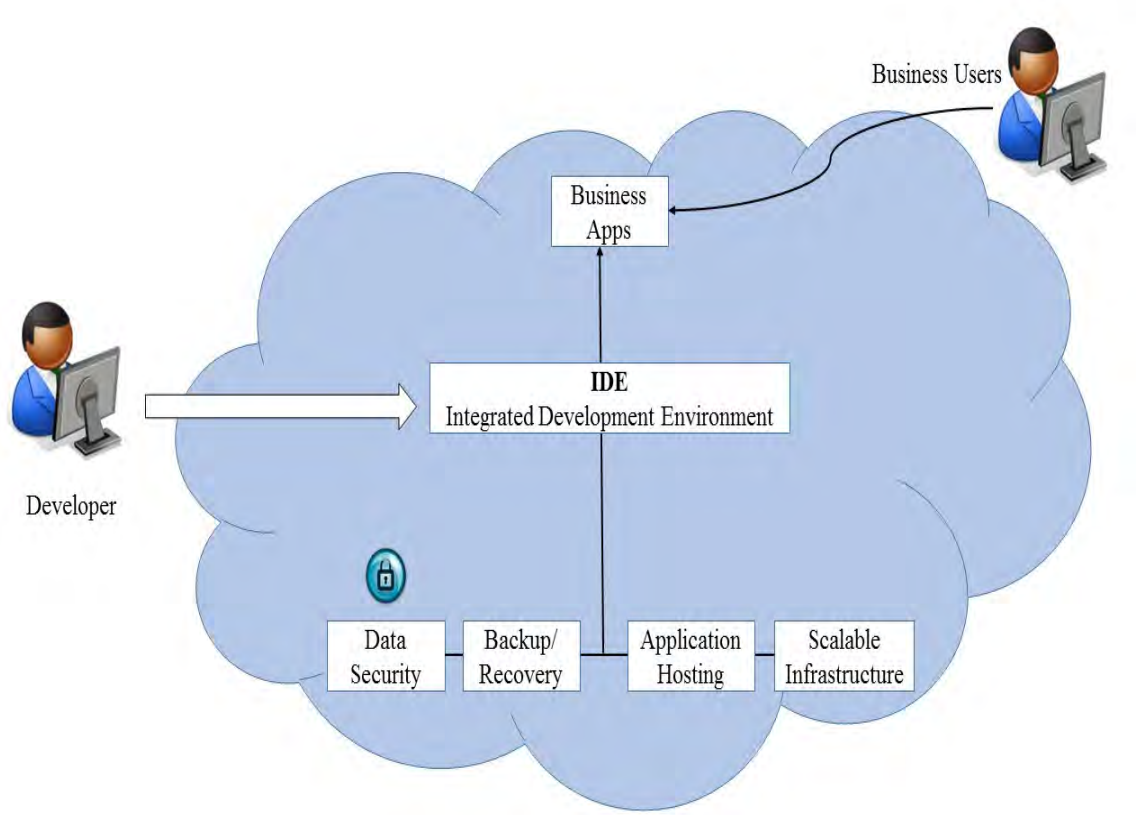


Figure 7. PaaS Model

3. Cloud Computing Benefits

Cloud computing is an important step toward an inexpensive means of universal accessing information and sophisticated computing resources (Antonopoulos & Gillam, 2010). Cloud computing promises increased financial savings coupled with expanded IT dexterity. The security benefits of the private cloud outweigh those of the public or hybrid cloud. The major benefits associated with cloud computing as defined by various scholars are as follows.

- Flexibility in Usage: The availability of immense computing and storage resources enables users to increase resources when in demand, thereby eliminating the need for adding more resources that remain underutilized (Armbrust, Fox, Griffith, Joseph, Katz, Konwinski, & Zaharia, 2010).
- Financial Benefits: Cloud computing allows expense organizing, payments for merely consumed services and resources, and savings from the reduction in IT personnel, hardware, software, maintenance, and management (Geczy et al., 2012).
- Functional Benefits: Since an organization's software applications are run on its cloud servers, software updates, patches, and required maintenance are all centrally administered (Geczy et al., 2012).
- On-demand Self-service: The consumer can singularly provision computing capacities, for example, server time and system stockpiling, automatic and as required without human collaboration with each CSP.
- Resource Management: Cloud computing gives a method for conveying and getting to enormously versatile shared assets on demand, progressively, and at moderate expense. (Rimal, Choi, & Lumb, 2010). It reduces overall expenses on maintaining and protecting data and allows the organization to save money on underutilized resources.

4. Cloud Computing Associated Risks

There are numerous concerns and risks associated with cloud computing. The most important risks are the three fundamental tenets of information security (i.e., the confidentiality, integrity and availability [CIA] triad). Confidentiality is the protection of data from unauthorized disclosure. This disclosure can either be accidental or intentional. Integrity is the assurance that a message or data received is in its original form, has not been modified, and is coming from a legitimate sender. Availability is the guaranteed access to data at all times without any delay, disruption or denial. Based on the CIA triad, the risks associated with cloud computing are expanded upon in the ensuing paragraphs.

Data Confidentiality and Security

All data rests with the cloud provider in unencrypted/readable form to facilitate data processing. Hence there are chances that data may be compromised and provided to an adversary against personal interests. Since the Internet is used to access data from cloud storage, it is more prone to attacks. Incidents like the Edward Snowden leaks in 2013 have also adversely affected the cloud industry. Unauthorized use of data in the cloud by any government or other intelligence agencies have raised serious concerns among cloud consumers.

Availability of Data

To ensure uninterrupted access to data, the cloud provider must guard against denial of service (DoS) attacks. Attacking a computer network with enormous floods of traffic and emails containing large attachment files can exhaust all resources and make it impossible for legitimate traffic to get through (Krutz & Vines, 2010). Since cloud consumers are relying on their CSP for data availability, cloud vendors must utilize highly resilient hardware and software techniques to ensure uninterrupted data availability.

Database Integrity

Database integrity is a very important aspect of cloud computing, as the prime mover for cloud computing is management of data and associated resources. If the database is not reliable or can be modified by an unauthorized user, results will never be fruitful and will eventually lead an organization toward failure. Session hijack attacks, man in the middle attacks, replay attacks, and others can also account toward an unreliable database.

TCP Hijacking and Social Engineering

While legitimate users are maintaining a connection with their cloud server, an attacker can hijack the TCP session and access the database. Similarly, various social engineering techniques can be employed by the attacker to capture the password or personal identification number (PIN) of the user for future use in manipulation of or access to the database.

Alignment and Integration

Enterprise architecture requires modification to meet the CSP model for optimum utilization, thus causing an organization to modify its enterprise architecture to meet the data formats, hardware interfaces, and so on.

Control of Data

Cloud computing is dynamic, with ubiquitous access to vast resources (Antonopoulos & Gillam, 2010). However, if the CSP faces a financial crisis, there are fair chances that hard drives from its data center will be sold on some online store like eBay or Amazon, thus causing consumers to lose control over their data.

Data Location

If the cloud provider stores data outside the territories identified in the service level agreement (SLA), serious concerns about the privacy and security of data may arise (Antonopoulos & Gillam, 2010). Additionally, if the data center is located at a place which experiences a natural disaster, complete loss of data and infrastructure may occur.

Trojan Horses and Malware

Emails containing Trojan horses and other malware from attackers can infect user machines. These Trojans or malwares can be programmed to silently transmit all data to the attacker when the user initiates connection with the cloud server.

C. CONCLUSION

Cloud computing is being adopted at various organizations and institutions to meet their IT needs, and organizations have saved considerable expenses on developing infrastructure, in addition to administering and maintaining software solutions. Cloud computing also allows organizations to access data worldwide and expand their international presence. This can be especially beneficial for organizations that lack the fnancial resources to establish costly data centers in foreign countries. There are, however, considerable risks associated with cloud computing. Although the private cloud is the most secure form of cloud computing, it is also the most expensive form as well. A majority of organizations are relying on a public or community cloud which is open to risks associated with data confidentiality, integrity, availability, and handling issues. However, with the use of various encryption techniques and use of the latest hardware for protection of data from eavesdropping, all concerns can be addressed.

THIS PAGE INTENTIONALLY LEFT BLANK

III. CLOUD COMPUTING IN PAKISTAN

In the previous chapter, the primary focus was on understanding cloud computing, its types and models, terms associated to cloud computing, and the benefits and associated risks of cloud computing. This chapter discusses the history of the information technology (IT) industry in Pakistan, developments in both IT and the industrial sector, the scope and use of cloud computing by private and government-owned industry, and local cloud service providers in Pakistan.

Pakistan's economy is based on agriculture and industry. After Pakistan achieved independence in 1947, the shortsighted vision of government coupled with poor economic policies resulted in varying approaches toward the industrial and technological sectors. Thus, Pakistan significantly lagged in acquiring the latest technology and tools to enhance development and improve its economy.

The IT industry in Pakistan started its journey after 1985, when the commercial usage of this technology was officially allowed. Recognizing the economic benefits of this sector, government leaders in Pakistan took concrete steps to support this industry, which resulted in tremendous investment from foreign and local industrialists. Besides formulating policies for increasing investments, the government took various other positive steps. These included allowing the industry to be exempt from taxes, providing fiber-optic connectivity at extremely low rates, developing the IT infrastructure, increasing human resource expertise in all fields, building a foundation for the software and hardware industries, restructuring the education sector, and hiring experts to increase intellect in the IT industry.

ISPs were issued licenses in 1995, and within the short span of five years, the Internet reached more than three million families (Ansari, 2012). With an Internet backbone of 130 Gbps, as of 2013 there are over 30 million Internet users in the country and over 1.7 million broadband users ("30m Internet users in Pakistan," 2013). As per the Pakistan Software Board, the IT industry's global share in the economy is estimated at

US$2.8 billion per year, with nearly 1,500 IT companies and a skilled workforce of 110,000 IT professionals (Pakistan Software Export Board, 2014).

While the IT industry has undergone a revolution, cloud computing has not yet established its firm roots in Pakistan. The Asia Cloud Computing Association's Cloud Readiness Index 2014 indicates that Pakistan is not among the top 15 countries in Asia where cloud services are being used optimally (Asia Cloud Computing Association, 2014). Index parameters for the Asia Cloud Computing Association report are data privacy, high speed Internet connectivity, data sovereignty, government regulatory environment and usage, reliable provisioning of power, protection of the intellectual property in data centers, and risks associated with data centers. Due to economic crises and a wave of terrorism in the country, Pakistan's government has been focused on fulfilling the basic necessities of its poor citizens. Further, the country's deteriorating law and order situation and lack of foreign investment in cloud computing has adversely affected the growth and development of the cloud computing industry. Notwithstanding the law and order situation and economic turmoil in the country, government leaders are poised to develop this industry. Cloud computing is already being used in the private and industrial sectors, but its adoption in the military has not been considered so far.

The climate of Pakistan's IT industry is conducive to providing the Pakistan Navy with an opportunity to develop its cloud computing capabilities while still relying on infrastructure and human resources inside the country. The Internet industry in Pakistan has evolved over time, leading to a significant number of commercial cloud providers. These commercial cloud providers have adopted a focused approach in developing this industry and have emerged as highly reliable providers for domestic organizations and firms. Moreover, commercial cloud providers in Pakistan are also providing cloud services to various other countries and multinational firms.

A. GOVERNMENT OF PAKISTAN-OWNED CSPS

Different cloud firms in the country are providing cloud services of various types and models to the private sector. Among these providers, Pakistan Telecommunication Limited (PTCL) is a government-owned company with a good reputation in delivering services related to cloud computing. Details about PTCL cloud services and the organization's infrastructure are provided in this section.

PTCL is a government-owned telecommunication corporation and is the pioneer in providing telephonic and internet services around the country. PTCL continues to retain a prominent position as a framework provider to other telecom industry and corporate clients in the country. PTCL maintains a mesh of optical fiber around all the major metropolitan cities of the country and is providing download/upload speeds from 1Mbps up to 50 Mbps. Besides providing landline telephone services and broadband internet, PTCL is also offering cloud services to its customers. Since PTCL is a government-owned corporation, all infrastructure/setup and data warehouses are located inside Pakistan. PTCL offers a public as well as a private model of cloud with servers starting from basic to enterprise. PTCL's standard server cloud package with standard disaster recovery support costs around US$10,500 per year.

The data center plays a pivotal role in an organization delivering cloud services. The Telecommunication Industry Association (TIA) and the American National Standards Institute (ANSI) have defined four levels of data centers. PTCL maintains a Tier III certified data center. These have multiple independent distribution paths, multiple types of IT equipment, and all equipment with multiple power sources. Tier III data centers maintain infrastructure with an expected availability of 99.982%, which is equivalent to a downtime of 94.608 minutes in one year. PTCL maintains data in storage area network (SAN) devices, which are considered highly reliable devices for accessing data online. Use of SAN devices help in accessing data at faster rates, provide 100% assurance of data availability, allow for isolation of data from other data on the same SAN device, and due to their scalability, require virtually no limit to store data (Hess, 2011). Due to the use of SAN devices, the PTCL cloud is highly scalable and flexible,

allowing for unlimited online storage and integration with native desktop environment to create and manage multiple cloud files.

PTCL provides the flexibility to its customers to utilize cloud services and pay for services only used by the firm. This gives the customer much flexibility in using cloud services and results in significant financial savings. PTCL cloud uses state-of-the-art hardware and provides disaster recovery for the protection of live workloads from a single point of failure. The disaster recovery facility gives assurance to cloud users for availability of enterprise data in case of loss or damage to primary data storage. The PTCL cloud is supported by team of experts with 24/7/365 availability.

PTCL, being a government-owned organization, has emerged as a highly reliable firm and is providing IT solutions to customers all across the country at considerably low rates. The PTCL data center with its large redundancies can be considered as the best among various competitors in the country. Since PTCL is a government-owned organization, it can be considered as a more reliable and trustworthy institution, and in case the Pakistan Navy decides to use cloud services from PTCL, additional data security and data encryption techniques can be put in place via a government channel.

B. COMMERCIAL CLOUD PROVIDERS

There are many private firms in the country that are providing cloud services in the commercial sector. Among these cloud providers, Cube XS Weatherly cloud services and Rapid Compute are among the best commercial cloud providers in the country. Details about these two firms are provided in the following paragraphs.

1. Cube XS Weatherly Cloud Services

In 2006, Cube XS Weatherly Cloud Services (CWCS), a privately owned firm, established the first Tier IV compliant data center in Pakistan. A Tier IV data center, in addition to meeting the Tier III data center requirements, contains features such as dual powered hardware, more cooling equipment including chillers, more fault tolerant data storage and distribution facilities, and an expected availability of 99.995%. An

availability index of 99.995% translates to a downtime of 26.28 minutes a year, which is 68.328 minutes less than for the Tier III data center.

In an environment where Pakistan is facing the worst power crisis of its history, CWCS provides highly reliable and uninterrupted services. Combined with physical and information security, CWCS claims to deliver an extremely safe and solidified environment that supports mission-critical business services (Cube XS Weatherly Cloud Services [CWCS], n.d.). Like PTCL and other cloud service providers, CWCS also provides SAN storage for its customers. Additionally, CWCS provides flexibility to its customers through pay-as-you-go cloud services and an optimized backup and disaster recovery strategy. CWCS maintains a highly competent workforce and support team that is available 24/7/365. CWCS offers IaaS and SaaS to its public cloud users, whereas it also offers private cloud to its customers. CWCS charges around US$1,400 per month for an enterprise level private cloud facility for an unlimited number of users (CWCS, n.d.).

CWCS is maintaining a superior Tier IV data center in comparison to the PTCL Tier III data center. However, besides its data center, CWCS is using similar IT infrastructure and storage devices as PTCL. Moreover, CWCS in comparison to PTCL charges more money for utilizing similar package of cloud services. Nevertheless, CWCS is a highly reliable and well reputed cloud firm that can be considered as a potential cloud provider for the Pakistan Navy.

2. Rapid Compute

Rapid Compute is another cloud service provider owned by a private firm, Cybernet, which was established in 1997 in Pakistan. The firm has a widespread network of its own fiber, making it one of the biggest ISPs in the country. Besides providing internet services, the company provides various IT solutions including cloud services to a large number of its customers. Rapid Compute is providing private and public cloud services with internet speeds in excess of 200 Mbps to its customers.

Further, a highly protected Rapid Compute data center is located inside Pakistan, which further enhances the confidence of its customers. Scalable, flexibility of paying as you go, disaster recovery infrastructure, and use of enterprise-class hardware makes

Rapid Compute a strong competitor in the market. Accelerating data using SAN devices results in delivering high performance for input/output operations. Rapid Compute owns a high performance and robust fault tolerant data center, which can allow its customers to access its data via either virtual local area network (VLAN) or virtual private network (VPN) secure connection. Higher data rates offered by Rapid Compute enhances a user's ability to upload and download data files in a secure VPN tunnel (Rapid Compute, 2014).

C. CONCLUSION

The cloud computing industry in Pakistan is under development, but it is anticipated that soon Pakistan's IT industry will lead the country's economy. Despite a poor start and the shortsighted vision in this sector, positive steps taken by the government have shown impressive results causing Pakistan's share in the global economy to increase to US$3 billion per year. PTCL, CWCS, and Rapid Compute have a strong infrastructure, wide coverage, and vast fiber-optic connectivity throughout the country. PTCL, CWCS, and Rapid Compute are reliable and have reputations of providing the best cloud services in the country. However, PTCL, as a government-owned organization, can be considered as the best option for using its services for the Navy. Furthermore, PTCL is providing cloud services at relatively cheaper rates than the commercial cloud providers mentioned above.

IV. DEVELOPING AN INTEGRATED FRAMEWORK FOR ADOPTING CLOUD COMPUTING

This chapter focuses on the U.S. cloud computing strategy, the NIST cloud computing guidelines and architecture, and the U.S. Navy's approach toward cloud computing. Deductions drawn from this discussion are used to lay out a framework for adopting cloud computing in the Pakistan Navy. IT is providing ever increasing capabilities to its users in the current geopolitical environment and despite the burdened economy, still consuming fewer resources than other technological sectors. Due to these capabilities and developments, IT ranks among the top revenue generating industries in the world. Cloud computing is among the world's leading IT solutions, and because of its enormous benefits, it is being adopted worldwide in commercial venues, government institutions, and defense organizations.

A. THE U.S. DOD CLOUD COMPUTING STRATEGY

Developments in the IT industry have steered in a novel epoch for the industrial sector and for the common man; however, numerous risks such as state-sponsored or independent cyber-attacks have called for a strong, secure, robust, and resilient IT infrastructure. To achieve improved mission effectiveness and enhanced cybersecurity, the DOD has taken various steps to build a reengineered information infrastructure and Joint Information Environment (JIE). These strides will convey speedier, more informed coordinated effort and choices empowered by secure, consistent access to data regardless of computing device or location (DOD CIO, 2012).

According to the DOD CIO, "cloud computing strategy is focused on moving the entire department from the current state of a duplicative, unwieldy, and expensive set of application silos to an end state of an agile, secure, and cost-effective service environment that can rapidly respond to changing mission needs" (DOD CIO, 2012). The cloud strategy promulgated by the DOD will have numerous benefits. Some of the benefits are shared information using common standards, consolidated cyber security, cost reduction in maintenance and operation of IT assets, data center standardization

allowing effective management as a single enterprise, and easy IT service management. Considerations for the DOD cloud computing strategy are cybersecurity, uninterrupted operations, information assurance (IA), and pliability. A highly resilient cloud infrastructure will have no single point failure and have minimum risk of downtime.

The DOD CIO is acting as a focal point and cloud broker for coordinating and implementing cloud computing throughout the DOD. The DOD cloud computing strategy explains the adoption of cloud in planned phases, ensuring coordination with all stakeholders at each transition phase. As defined in the DOD cloud computing strategy, the transition to the DOD cloud has been divided into the following four phases

- Foster adoption of cloud computing
- Optimize data center consolidation
- Establish the DOD Enterprise Cloud Infrastructure
- Deliver Cloud services (DOD Cloud Computing Strategy, 2012).

(1) Foster Adoption of Cloud Computing

The DOD cloud represents a cultural shift to change the DOD from a coalition of divisions and organizations with their mission-specific arrangements of frameworks, procedures, administration, and controls to a more consistent, enabled, incorporated, and information driven data environment (DOD CIO, 2012). Adoption of cloud computing in the DOD is governed under the authority and policies promulgated by the DOD CIO. The DOD cloud has transformed the information-sharing environment to include common standards, consolidated cybersecurity, continuity of operations, information assurance, flexibility, and centralized governance (DOD CIO, 2012).

The DOD CIO took several steps to adopt cloud computing in the department, including reducing operating and maintenance costs, eliminating acquisition complexities, shifting the focus to consuming IT resources rather than acquiring and managing, and publishing new policies. The DOD CIO is entrusted with identifying consumers of cloud services and coordinating with other stakeholders to increase the visibility of these services throughout the department. Moreover, the DOD CIO is tasked with promulgating the best practices for adopting cloud computing including acquisition, security, and identification of evolving technologies (DOD CIO, 2012).

(2) Optimize Data Center Consolidation

The DOD cloud computing strategy focuses on consolidating all data centers to achieve savings in manpower, acquisition, and operating costs, and enforce strong security measures for the protection of networks from cyber-attacks. Consolidation of data centers is expected to provide standardizations among all center users and enable effective management as a single enterprise (DOD CIO, 2012). All organizations and stake holders within the DOD are allowed to operate their own data centers. However, these organization are obliged to work as indicated by standard operational, business, and IT service management processes. This will guarantee their capacity as a single, legitimately consistent computing environment meeting all necessities for agile failover, fiasco recuperation, progression of operations, security, strength, and load balancing (DOD CIO, 2012).

(3) Establish the DOD Enterprise Cloud Infrastructure

The DOD is responsible for providing an enterprise cloud infrastructure for all its components and has designated the Defense Information Systems Agency (DISA) as a cloud broker. The DOD is relying on the DISA for easier and safer cloud services as the cloud infrastructure belongs to a variety of departments and as the cloud services are being provided by federal as well as commercial providers. A key element of the DOD cloud computing environment is that it gives a very versatile processing environment that does not have a single point of failure; the break-down of one node in a framework in a cloud domain has no effect on data accessibility, diminishing the danger of perceivable downtime (DOD CIO, 2012).

A cloud broker having a technical and administrative aspect is required to operate optimally, provide synchronized delivery of cloud services, and integrate multi-provider cloud environment. Thus, designating the DISA as a cloud broker provides the DOD with an opportunity of centrally monitoring all cloud service providers' performance and ensures cybersecurity measures are optimally in place as per the enforced standards among all stakeholders. The DISA ensures compliance of all information assurance requirements of the DOD, increases the ease of encryption and key management for

secure cloud services, enables an integrated cyber intrusion and detection system, and provides a common entry point into the cloud (DOD CIO, 2012).

(4) Deliver Cloud Services

The DOD cloud infrastructure is dedicated to delivering secure, reliable, integrated, and cheaper cloud services to all its departments and stakeholders. The policies promulgated by the DOD CIO for fostering adoption of cloud computing, consolidating data centers, and establishing the DOD enterprise architecture are integrated with each other. Further, departments and agencies across the DOD are also being encouraged to adopt commercial cloud providers that are in-line with their specific mission requirements.

B. NIST CLOUD COMPUTING REFERENCE ARCHITECTURE

The NIST reference architecture defines "a conceptual model comprised of abstract architectural elements and their interactions with cloud computing actors, systems components, and their unique arrangement to deliver computing services, management functionalities required to support the life cycle of operations, and other aspects such as security and privacy" (NIST, 2011c).

In Figure 8, the cloud carrier is acting as a backbone and interconnects the cloud consumer, cloud auditor, cloud provider, and cloud broker. The cloud consumer uses cloud services from the cloud provider, and the cloud broker acts as a service intermediator, service aggregator, and service arbitrage. Besides providing cloud services, the cloud provider is also responsible for the integration of various components of these services. According to NIST, "These components include security and privacy arrangements; cloud service management that includes business support, configuration, and interoperability; service orchestration at cloud service layers, which refers to the arrangement of system components to support provider activities in arrangement, coordination, and management of computing resources depending on type of service chosen among SaaS, PaaS, and IaaS" (NIST, 2011c); and resource abstraction. The cloud auditor independently oversees security, privacy, and performance of cloud services.

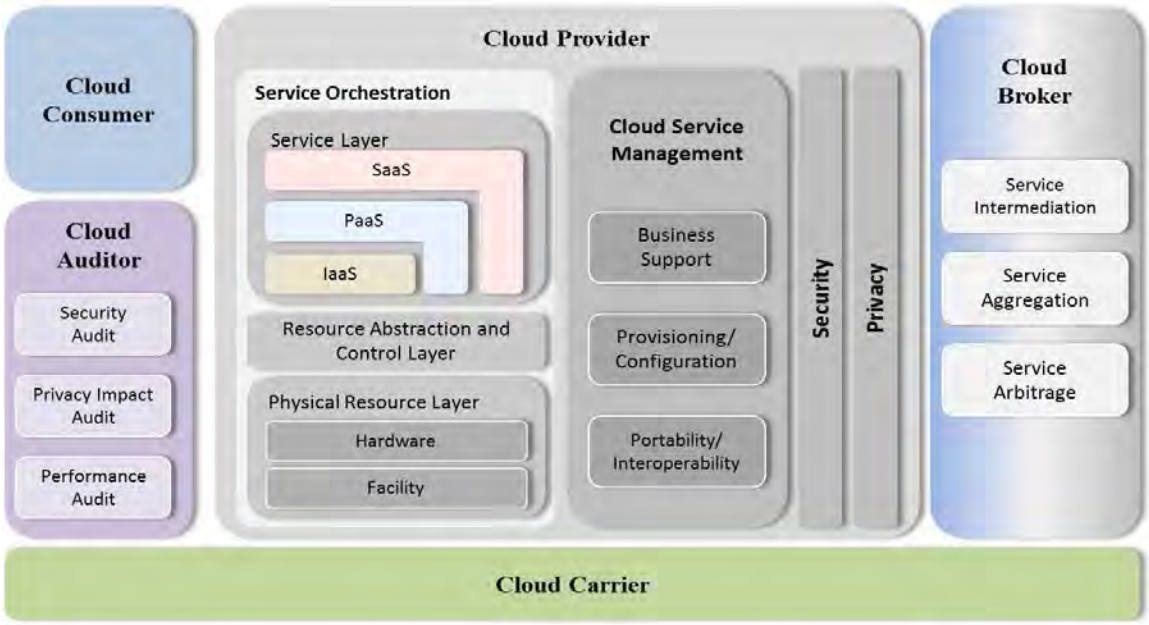


Figure 8. NIST Cloud Computing Reference Architecture (from NIST, 2011a)

In a cloud based atmosphere, both the cloud provider and cloud consumer share the regulation of assets. Control over the computational resources varies with respect to the service model chosen for cloud services. Figure 9 illustrates a typical software pile representation indicating the application, middleware, and OS layers (NIST, 2011c). Critical analysis of the delineation of control over the operating system layer helps in understanding the responsibilities of stakeholders involved in managing the operating system layer. Software for end users are contained in the application layer, and these applications are used and maintained by SaaS consumers (NIST, 2011c).

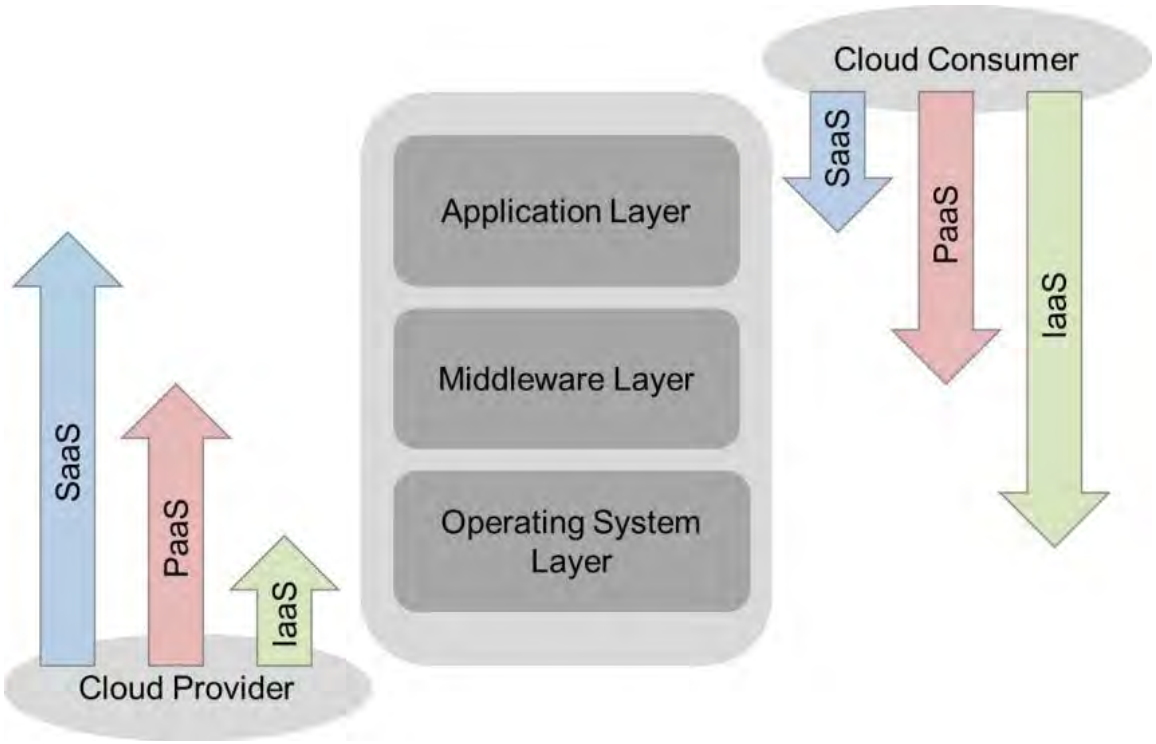


Figure 9. Scope of Control between Cloud Provider and Consumer (from NIST, 2011c)

The NIST (2011C) has identified three reference architectures for adopting cloud computing. These architectures are focused on providing cloud services to the cloud consumer via a cloud broker as an intermediary, a cloud provider delivering cloud services through an independent cloud carrier, and a cloud consumer receiving cloud services from a cloud provider while a cloud auditor carries out an independent audit of cloud services.

(1) Scenario 1

In Scenario 1 of the NIST reference architecture shown in Figure 10, the cloud broker is acting as an intermediary, arbitrager, and aggregator. It has an SLA for cloud services with a cloud provider. The cloud broker is also responsible for ensuring availability of cloud services to the cloud consumer and resolving concerns related to the cloud carrier. Cloud services are delivered to the cloud consumer by the cloud broker through another SLA. The cloud consumer is not maintaining direct contact with the

cloud provider and completely relies on the cloud broker for maintaining quality of services, security, privacy, and data availability.

In Scenario 1, the cloud broker is receiving cloud services from the cloud provider and then delivering these services to the cloud consumer. Thus, the cloud consumer will have to rely on a commercial vendor for cloud services. If the Pakistan Navy adopts the architecture in Scenario 1, then it will be required to keep its data at servers under the administrative and operational control of commercial cloud vendor. This increases the probability of data compromise or misuse. Due to the operational requirements of the Navy, uninterrupted access to cloud services is essential, which may become doubtful if the cloud carrier is having large downtime or if more than one point of failure exists in infrastructure.

Figure 10. Scenario 1 (from NIST, 2011a)

(2) Scenario 2

Juxtaposed to Scenario 1, in Figure 11, the cloud consumer is receiving cloud services directly from cloud provider. There is no intermediary or cloud broker between the cloud consumer and the cloud provider. The cloud provider arranges the cloud carrier, which can provide an encrypted and uninterrupted connection to cloud provider and cloud consumer. The cloud provider arranges two SLAs for delivery of cloud services, one with the cloud consumer and one with the cloud carrier. Providing uninterrupted and secure access to cloud resources is the responsibility of cloud provider. However, since the channel connecting the cloud consumer and the cloud resources is not under the control of the cloud consumer, the risk of data being compromised or eavesdropped by an attacker is very high.

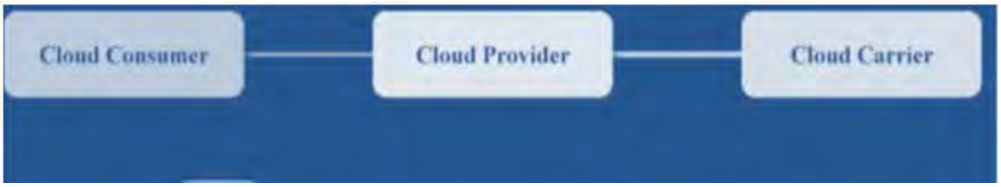


Figure 11. Scenario 2 (from NIST, 2011a)

(3) Scenario 3

In Scenario 3 of the NIST reference architecture, the cloud consumer is using cloud services from the cloud provider. Thus, in Figure 12, the cloud provider is responsible for delivering uninterrupted, secure, and reliable cloud services to the cloud consumer. An independent entity, a cloud auditor, carries out an assessment of security, privacy, and quality of services being provided to the cloud consumer. In this model all unclassified data can be kept at the servers of the cloud provider with an agency similar to the DISA. The Pakistan Navy can act as a cloud auditor and audit the services being offered by the cloud provider.

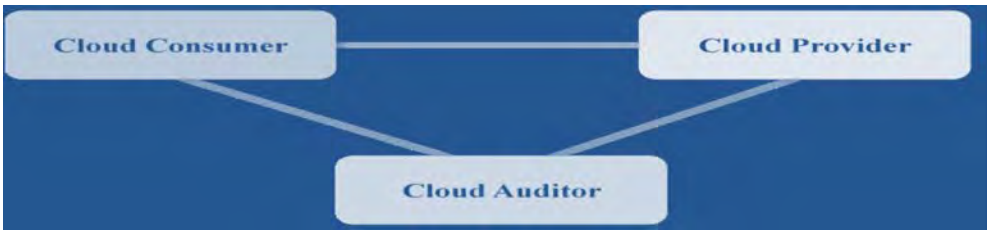


Figure 12. Scenario 3 (from NIST, 2011a)

C. THE U.S. NAVY APPROACH TOWARD CLOUD COMPUTING

The U.S. Navy, the DOD, and the DISA are collectively working on adopting cloud computing for the U.S. Navy. Based on the importance and benefits of cloud computing, the U.S. Department of Navy (DON) published its updated cloud computing strategy in June 2013. Adoption of cloud computing by the U.S. Navy will accelerate mission planning and execution of expeditionary missions (Corrin, 2014). The U.S. Navy has designated the DISA as an Enterprise Cloud Service Broker to layout the methodology for adopting cloud computing. The strategy is aimed at reducing overall IT

expenditures, reducing the number of data centers to minimize operational and maintenance costs, and using alternative means to provide cloud services to its users. The key points of the U.S. Navy cloud computing strategy includes certifying and accrediting all systems and hardware being used for the Navy cloud; identifying commercial cloud providers for low impact data; identifying security, privacy, and encryption related requirements; defining the role of the DISA for the U.S. Navy cloud; and maintaining and operating classified database cloud services (Department of Navy Chief Information Officer [DON CIO], 2013).

(1) Certification and Accreditation

As a first step, the DON deputy CIO is required to ensure that all systems used throughout the DON are appropriately verified and correctly accepted by the appropriate Designated Approval Authority. This will give the DON CIO assurance that all hardware and infrastructure being used for providing cloud services is reliable and can withstand cyber-attacks from an adversary, and minimize chances of having back doors in hardware for eavesdropping by an attacker.

(2) Identifying Commercial Cloud Provider

In order to move DON low impact information, which is publicly accessible information, applications, and websites containing information approved for public release to commercial cloud service providers, the DON cloud broker, the DISA, is to identify cloud service providers that meet mission and security requirements dictated by policies promulgated by the DOD and other agencies. Furthermore, in order to achieve the objective of cost savings within the DON, the DON cloud broker is to analyze alternatives and evaluate commercial, federal, and DOD solutions to identify the most cost-effective holding atmosphere for medium impact systems.

(3) Identifying Requirements

The DON deputy CIO is required to assist the DON cloud broker, the DISA, in accurately capturing the requirements for providing cloud services including those related to security, privacy, encryption, and bifurcating data in impact levels as identified by the DOD cloud security model. Correctly categorizing the data as per impact levels is a very

sensitive task, and any inadvertent mistake can result in high-impact–level data appearing on a low-impact cloud server or vice versa, which will ultimately result in a security and privacy breach.

(4) Role of the DISA

The DISA has been given the responsibility of acting as a cloud broker for the DON. The DISA is required to lay out an enterprise architecture model for the DON. This enterprise architecture model is focused on integrating all components of the DON in an environment for a quick, secure, reliable, and easily accessible pool of resources and for providing up-to-date information to war fighters. Moreover, in response to the DOD cloud computing strategy and the DON cloud computing strategy, the DISA is required to identify commercial cloud providers that are able to provide cloud services for the low-impact unclassified data to the DON. While contracting with commercial cloud vendors, the DISA is to ensure that all requirements identified by the DOD and other agencies for security, privacy, and encryption of data are met.

(5) Classified Data

The DON cloud computing strategy clearly indicates that all classified data that is not cleared for public release will be maintained in data centers owned by the U.S. Navy. Although the primary focus of the DON cloud computing strategy is to reduce the overall IT expenses within the department, maintaining security and protection of classified and sensitive information is paramount. Thus, only unclassified and low-impact information is being kept at a commercial cloud provider, and for all sensitive and classified information, data centers will be operated and maintained by the Navy.

A critical analysis of the U.S. Navy strategy for adopting cloud computing indicates that the primary focus is on integrating all departments, cutting expenses incurred through maintaining and running IT assets, and providing up-to-date and correct information to its war fighters and decision makers. Adopting cloud computing will shift the U.S. Navy away from a client–server model and in terms of its maritime assets, will provide the flexibility to access pools of data more reliably and securely. In March 2014, the U.S. Navy shifted its public-facing unclassified data to Amazon Web Services

(AWS). According to U.S. Navy CIO Terry Halvorsen, this shift will save the Navy around 60% of its spending in managing data at its own data center (Verge, 2014). Further, the U.S. Navy presently maintains around 150 data centers, and the CIO of the U.S. Navy aims to bring them down to 25 or less (Verge, 2014). Use of AWS for unclassified low-risk information will result in an overall reduction in expenses and provide an opportunity to more sturdily focus on protecting classified information flowing over the information channels.

D. FRAMEWORK FOR THE PAKISTAN NAVY

Analysis of the DOD cloud computing strategy, the NIST reference architecture for cloud computing, the U.S. Navy cloud computing strategy, and existing IT and human resource infrastructure in Pakistan reveals that none of these models can be adopted as a whole. However, to formulate a strategy for adopting cloud computing in the Pakistan Navy, an integrated framework having input from all these models is required. The decision as to which model best suits the Navy's requirements will be based on three factors: user needs, the cloud carrier being selected, and the classification of information.

To foster the adoption of cloud computing in the DOD, the DOD CIO is required to identify potential consumers of cloud services and ensure coordination with other stakeholders to increase the visibility of these cloud services throughout the department. Similarly, the U.S. Navy cloud computing strategy emphasizes identifying the correct number of cloud consumers for the U.S. Navy cloud. This will facilitate designing an overall enterprise architecture for the U.S. Navy as well as for the DOD. Thus, as a first step to adopting cloud computing in the Pakistan Navy, potential consumers of the cloud services must be identified in order to develop an effective and synergetic framework of cloud services.

The DOD cloud computing strategy and the U.S. Navy cloud computing strategy are focused on minimizing IT expenditures, reducing data centers, and using alternative means to provide cloud services to its users. Moreover, segregating high-impact information from low-impact information is also a key point in the U.S. Navy cloud computing strategy. Bifurcation of classified data from low-impact unclassified data will

allow for the flexibility to use commercial cloud vendors for unclassified data. Cloud brokers of the U.S. Navy and the DOD are required to verify the hardware and infrastructure used by the commercial vendors and to ensure that they meet security and privacy requirements. Thus, as a second step in the case of the Pakistan Navy, bifurcating classified and unclassified data will ultimately help in following a strategy similar to that of the U.S. Navy and the DOD and will minimize IT expenditures for unclassified data.

The DOD and the U.S. Navy cloud computing strategies aim to shift the environment of the departments from maintaining hardware and infrastructure to increasing mission effectiveness and operational efficiencies. Thus, use of commercial cloud providers for unclassified data as well as use of a private cloud for high impact and sensitive data translates into a hybrid model of cloud computing. As is the case with the U.S. Navy, as a third step the Pakistan Navy also needs to identify the best suited model for adopting cloud computing based on its requirements and policies.

The cloud carrier acts as an intermediary and is required for accessing cloud services from a cloud provider. The U.S. Navy makes use of several channels for the exchange of classified and unclassified information, including satellite over oceans and terrestrial communication networks over land. Although in the U.S. Navy and the DOD cloud computing strategy, selection of a cloud carrier is not considered due to the existence of strong communication infrastructure, its importance for the Pakistan Navy cloud is paramount. Thus as a fourth step toward the framework for the Pakistan Navy cloud, selection of a cloud carrier for use of cloud services over oceans needs emphasis and deliberation.

In order to launch cloud services for the Pakistan Navy, besides having command structure to implement this technology, it is paramount to develop a fully integrated, robust, secure, and efficient infrastructure that can deliver uninterrupted cloud services to the consumers.

Based on this discussion, a recommended framework for developing a model of cloud computing for the Pakistan Navy can be based on following steps.

1. Identify cloud consumers within and outside Pakistan Navy
2. Bifurcating classified and unclassified data
3. Identify cloud model
4. Identify cloud carrier
5. Launch cloud services

E. CONCLUSION

The U.S. Navy and the DOD cloud computing strategy is aimed to provide a highly resilient, secure, reliable, quick, and integrated solution to increase mission effectiveness and operational efficiency of its warfighters. This thesis has laid out a framework for adopting cloud computing for the Pakistan Navy based on input from the U.S. Navy, the DOD cloud computing strategy, and the NIST architecture. This framework is focused on enhancing information sharing, increasing economy of efforts, advancing reliability of IT infrastructure, and eliminating over-expenditures in the IT domain. Moreover, this is a generic framework that can be adapted to develop a cloud infrastructure for the Navy. Shore-based and sea-based components of the cloud infrastructure will require an integration, as the sea-based cloud setup will be focused on tactical features of the cloud in contrast to shore-based, which will be more inclined toward administrative setup.

THIS PAGE INTENTIONALLY LEFT BLANK

V. CLOUD COMPUTING IN PAKISTAN NAVY

The Pakistan Navy, since its birth in 1947, has been struggling to strengthen its fleet and transform it into an invincible force comprised of modern warships, aircrafts, submarines, and other assets. The Pakistan Navy's role is to defend the sea lines of communications for the country. This includes providing uninterrupted movement of merchantmen/trade and protecting the entire coast, which stretches around 1,000 km. Despite the fact that more than 95% of the country's trade is transported over sea, the Navy is the smallest force in size, as compared to the Pakistan Army and the Pakistan Air Force. Due to globalization, world economies are progressively becoming interdependent, which is likely to further boost seaborne trade for Pakistan. Based on the current financial crisis of the country and the limited size of its economy, the Pakistan Navy receives the lowest priority, and its share in the military budget is significantly less than sister services.

The Pakistan Navy is a small to medium size force with the role of protecting sea frontiers, of deterring any aggression at and from the sea, and of protecting sea lines of communication. Besides these roles, the Pakistan Navy operates around the world for the multinational maritime exercises, for anti-piracy operations, for coalition maritime campaign plan operations, for disaster relief operations, for humanitarian support, for flag showing, and for contributing to international efforts of maintaining good order at sea. Thus, considering operations of the Navy and concerns related to privacy, security, and availability of data, a customized cloud architecture for the Pakistan Navy is considered the best viable option.

Remaining within limited resources, equipping the Navy with the latest technology, and strengthening seaward defense has always been a top priority of the naval headquarters. The Pakistan Navy's recent inductions of indigenously built frigate and fast attack craft and its launch of a fleet oiler at Karachi Shipyard and Engineering works are manifestations of the Navy's commitment toward excellence. The technological base of Pakistan is limited, and the Navy often has to rely on foreign vendors for addressing its technical issues. However, concrete steps are being undertaken

to improve the overall technological status of the Navy. In pursuing this aim, the Pakistan Navy is endeavoring to modernize its information-sharing infrastructure and to adopt the latest global methodologies for the rapid exchange of information at all times. The previous chapter discussed the U.S. DOD cloud computing strategy, the NIST reference architecture for cloud computing, and the U.S. Navy approach toward cloud computing. Based on the inferences drawn from these models and the requirements of the Pakistan Navy, an integrated framework for adopting cloud computing was proposed. In this chapter, the proposed framework is discussed in further detail.

A. ADOPTING CLOUD COMPUTING IN THE PAKISTAN NAVY

Before adopting cloud computing in the Pakistan Navy, there is a need to develop a command structure that will act as a cloud broker on behalf of the Pakistan Navy and will build an enterprise architecture supporting consumers within and outside the Navy. Designating a cloud broker can help the Navy standardize its IT infrastructure, protocols, and procedures for sharing information throughout the department. Further, a cloud broker can provide the Navy an opportunity to save money being incurred on manpower, cybersecurity, and operating costs.

Besides identification of the cloud consumers, bifurcating classified and unclassified data provides flexibility and allows the Navy to use private firms for hosting unclassified data. Selecting the correct cloud model as per the requirements of the Navy and a cloud carrier for use of cloud services overseas is paramount in order to launch cloud services for the Navy. The proposed integrated framework for adopting cloud computing in the Navy consists of five steps.

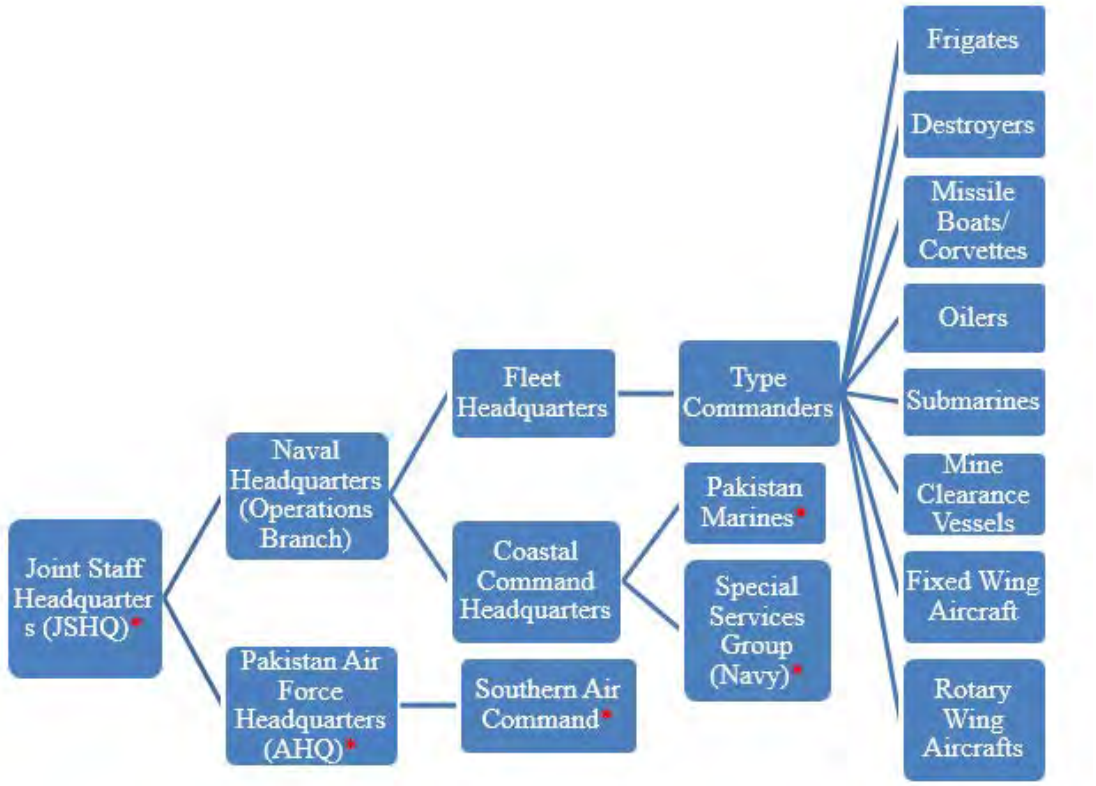
1. Identify cloud consumers within and outside the Pakistan navy
2. Bifurcating classified and unclassified data
3. Identify cloud Model
4. Identify cloud carrier
5. Launch cloud services

1. Cloud Consumers for the Pakistan Navy

The Pakistan Navy is a diverse and four-dimensional force comprised of surface, sub-surface, and air platforms. Besides acquiring platforms from the United States, the UK, France, and China, the Pakistan Navy also operates its own built frigates, corvettes, missile craft, and submarines. Thus, the combination of different platforms and military hardware makes the Pakistan Navy an effective and potent force in the region. As is the case with the U.S. Navy's cloud computing strategy, the correct identification of cloud consumers will help in building an accurate enterprise architecture. Not all consumers need access to all information spread over the complete spectrum of classification at all times. The Pakistan Navy should consider its present inventory of the fleet and infrastructure ashore with the aim of providing the right information to the right platform at the right time. Tables 1 and 2 includes potential consumers of the cloud services based on consumers' role and need to access operational and non-operational data.

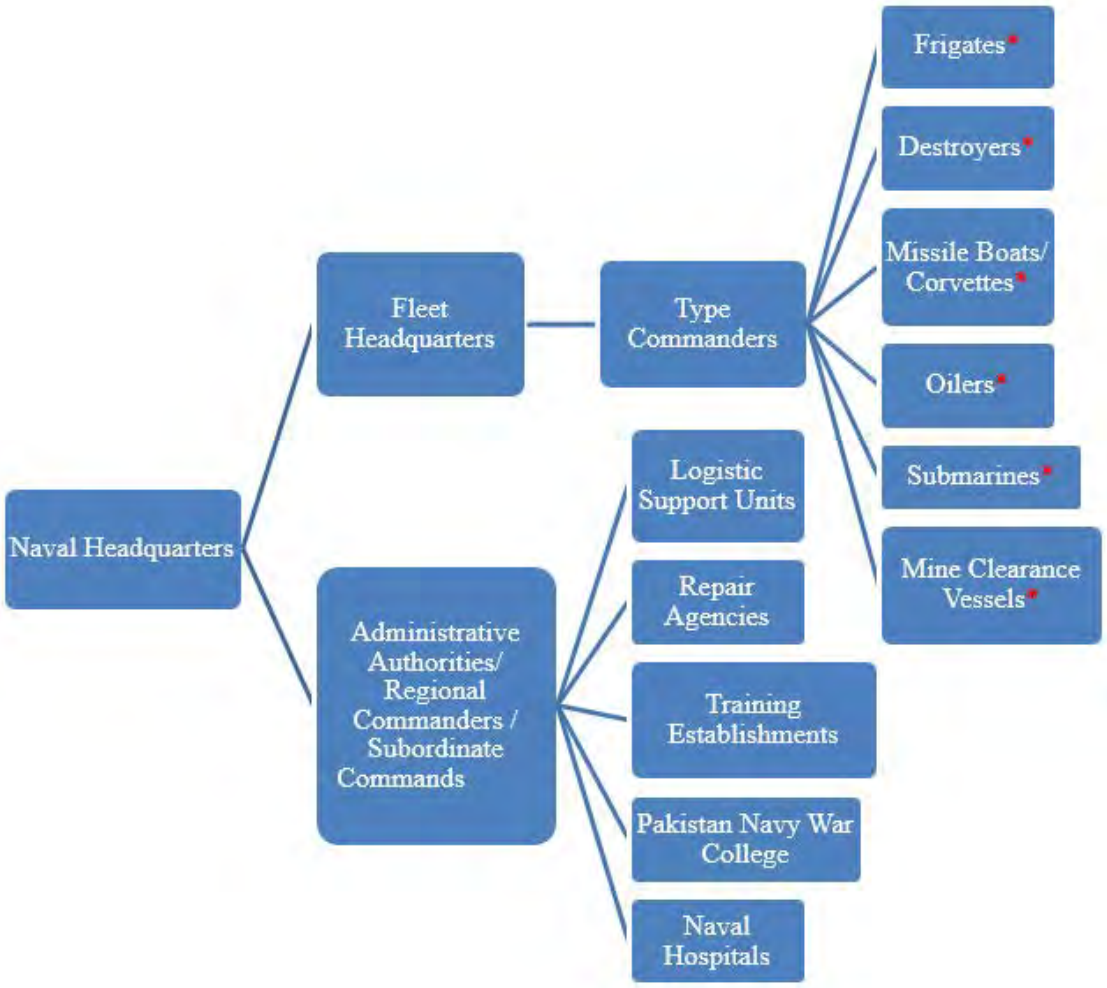
Cloud consumers marked with an asterisk in Tables 1 and 2 are potential customers of operational and non-operational data based on their involvement in the mission. Since the Pakistan Navy does not own and operate fighter aircrafts for missions at sea, the services of the Pakistan Air Force are requested for undertaking such missions. Thus, the Pakistan Air Force is a strong candidate for becoming a cloud consumer of operational data of the Pakistan Navy. Similarly, the Special Services Group of the Navy and the Pakistan Marines undertake missions in support of the Pakistan Navy both afloat and ashore, making them a viable cloud consumer of operational data. Access to the non-operational data to the selected fleet units will ease the burden on limited bandwidth available for exchange of information at sea.

Table 1. Cloud Consumers—Operational Data



* Requirement-based access

Table 2. Cloud Consumers—Non-operational Data



* Requirement-based access

2. Bifurcation of Classified and Unclassified Data

In an operational environment, enormous amounts of data flow between a variety of afloat, airborne, submerged, and ashore units. Therefore, it is prudent to bifurcate data based on its classification. A dividing line between classified and unclassified information will help to design an architecture that can protect classified information from being compromised from the cloud server. The U.S. Navy's cloud strategy focuses

on adopting private firms for unclassified data. Thus, bifurcating classified and unclassified data will ultimately provide the flexibility to use commercial cloud providers in Pakistan for hosting unclassified data for the Navy. Furthermore, this will eliminate the chances of data spillage, which occurs when classified data moves into unclassified data servers. Responsibility for precisely bifurcating data before putting it on a cloud server lies with the cloud consumer, in this case on the Pakistan Navy, to avoid inadvertent spillage over the unclassified data channel.

3. Identify Cloud Model

The use of cloud computing for achieving military objectives is not a unique idea. Many militaries around the globe have adopted different models of cloud computing based on their individual needs. Some factors that are considered include force size, structure, and composition; diversity of operations; in-house technological base and expertise; technical support; the capability to operate and maintain technology; and financial support available.

Based on the needs of an organization and resources available, there are three basic models for adopting cloud computing, each having different pros and cons. To decide which model best suits the Pakistan Navy requirements, various factors are considered. These factors include the spectrum of operations of the Navy, potential consumers of the cloud services, sensitivity of the data, confidentiality, integrity, and availability of data; technological base available in the country; human resources available to build and operate this technology; the NIST reference architecture model; and the financial resources available. In order to address all the requirements of the Pakistan Navy and other security concerns, two different cloud models can be adopted by the Pakistan Navy. A private cloud owned by the Pakistan Navy could be used for all classified data (operational and non-operational), and a public cloud from a commercial vendor could be used for all unclassified data (operational and non-operational). The use of a private firm for unclassified, low-risk information by the Pakistan Navy will result in an overall reduction in expenses and will provide the opportunity to focus on protecting classified information flowing over the information channels. Responsibility for ensuring

smooth, uninterrupted, secure, and standardized flow of information to all assets (i.e., ashore, afloat, and submerged) can be entrusted to the cloud broker for the Pakistan Navy. Moreover, in consonance with the U.S. DOD cloud computing strategy, data centers for classified and unclassified data may be built according to standard service management processes, creating a single seamless computing environment. All requirements for graceful failover, disaster recovery, continuity, security, resiliency, and load balancing would be met.

4. Identify Cloud Carrier

The cloud carrier is considered the backbone of cloud services. It helps the cloud consumer access data uninterruptedly from remote locations. A reliable cloud carrier provides assurance to the consumer that data is not compromised, modified, or blocked while it is in transit (i.e., provides confidentiality, integrity, and availability). Furthermore, bandwidth provided by cloud carrier will determine the speed with which data, including video streams, can be downloaded and transferred between operational units and headquarters. In case of afloat units at sea, bandwidth limitations are more severe as data is transferred over satellite. Thus, identifying the cloud carrier is very important and needs deliberation.

In Pakistan, various commercial vendors are providing services as cloud carriers with speeds in excess of 1GB/s, however, at present none of these firms have their fingerprints overseas and own a satellite. Thus, the Pakistan Navy will have to rely on international vendors for the use of afloat cloud services. At present, various international firms are providing such services in Pakistan; however, using a commercial satellite link for exchanging classified information is not a viable solution. Notwithstanding the risks associated with a commercial satellite channel, until the time when Pakistan launches its own satellite for military communication, various encryption techniques can be adopted. Dedicated channels similar to the U.S. Non-secure IP Router Network (NIPRNet) and the Secure IP Router Network (SIPRNet) can be formed to access cloud services over land. As an alternative to using SATCOM for exchange of information between units at sea and at land, worldwide interoperability for microwave access (WiMAX) can be used to

maximize range coverage and minimize expenses being incurred on SATCOM. Appendix A covers more details on using WiMAX as an alternate to SATCOM.

5. Launch Cloud Services

Cloud services can be launched after identifying the best suited cloud model, identifying potential consumers, identifying a cloud carrier to access resources, and bifurcating classified and unclassified data. However, adopting cloud computing is not as simple as these four steps suggest. Strong IT infrastructure, human resources for management and operation, building data centers, defining security protocols, and building data nodes on all operational units including ships, submarine, and aircraft, is a daunting task. In order to enhance human resource capital in IT for running cloud services for the Navy, it is considered prudent to provide opportunities to individuals to undergo training at reputed cloud providers in the country. Training should focus on maintaining, operating, and providing necessary security measures to avoid a data breach. Additionally it is important to develop a culture that will help transform the traditional way of sharing information and resources to a modern way of accessing information remotely via the Internet. A culture for using the Internet to exchange information will grow rapidly if the consumers trust the technology and there are no interruptions or delays. Thus, the Pakistan Navy may begin with cloud computing by adopting this technology initially at smaller scale and as the system is matured, may enhance it to all over the Navy.

B. CONCLUSION

The Pakistan Navy has continuous presence in the Indian Ocean and is successfully contributing to fighting the menaces of terrorism, piracy, and human trafficking and to maintaining good order at sea. Given that the Pakistan Navy is undergoing development and modernization in order to conduct maritime operations with greater vigor, easy and rapid access to information is paramount. Adopting cloud computing will allow the Navy's warfighters to rapidly exchange information with each other without having constraints on bandwidth and resources. Establishing a cloud broker similar to the U.S. DISA will help in developing enterprise architecture. Implementing

two different cloud models will help in developing infrastructure and minimizing operating costs. Further, the bifurcation of information over the cloud will eliminate the chances of compromising classified data over an unclassified network. This will also ease the traffic flow of operational data over classified channels. Since none of the commercial vendors in Pakistan have a footprint overseas, international satellite bandwidth providers may be hired. The use of encryption over satellite channels may be considered for maintaining the confidentiality of data.

THIS PAGE INTENTIONALLY LEFT BLANK

VI. CONCLUSION

A. SUMMARY

This thesis expresses the importance of cloud computing in today's rapidly advancing technological world and the need to enhance information sharing among all the stakeholders within and outside the Pakistan Navy. To formulate a strategy for adopting cloud computing in the Pakistan Navy, a literature review was carried out to understand related concepts, definitions, and terminologies; various cloud models; different architectures of cloud computing; IT infrastructure in the country; commercial cloud providers; and information-sharing infrastructure within the Pakistan Navy. Although the cloud computing industry in Pakistan is still under development, it is anticipated that this sector will soon lead the country's economy and help generate significant revenue.

This thesis has laid out a framework for adopting cloud computing following an in-depth analysis of various cloud models including the NIST reference architecture for cloud computing, the DOD strategy for adopting cloud computing, and the U.S. Navy's road map toward cloud computing vis-à-vis associated benefits and risks. The proposed framework is focused on enhancing information sharing, increasing economy of efforts, advancing reliability of IT infrastructure, and eliminating over-expenditures in the IT domain. Thus, to provide a highly resilient, secure, reliable, quick, and integrated solution to increase mission effectiveness and operational efficiency of warfighters, the following steps are recommended for adopting the cloud computing in the Pakistan Navy:

1. Identify cloud consumers within and outside Pakistan Navy
2. Bifurcating classified and unclassified data
3. Identify cloud Model
4. Identify cloud carrier
5. Launch cloud services

As is the case with the U.S. Navy's cloud computing strategy, the correct identification of cloud consumers will help in building an effective enterprise architecture and providing the right information to the right person at the right time. Bifurcating classified and unclassified data can help the Navy in designing an architecture for

protection of classified information and will also provide flexibility in using commercial cloud providers identified in the thesis for unclassified information. While selecting a cloud model for the Pakistan Navy, various factors have been considered. These include spectrum of operations of the Navy; potential consumers of the cloud services; sensitivity of the data; confidentiality, integrity, and availability of data; the technological base available in the country; the human resources available to build and operate this technology; the NIST reference architecture model; and the financial resources available. Thus, to address all the requirements of the Pakistan Navy and other security concerns, two different cloud models are recommended for the Pakistan Navy. A private cloud owned by the Pakistan Navy would be used for all classified data (operational and non-operational), and a public cloud from a commercial vendor would be used for all unclassified data (operational and non-operational).

A reliable cloud carrier is considered very important to access cloud resources over the Internet. Since the Pakistan Navy does not own its own military communication satellite and none of the cloud providers in the country have footprints over the ocean, the Navy will have to rely on an international vendor. In order to maintain the confidentiality, integrity, availability of data (classified and unclassified), and its protection from eavesdropping, various encryption techniques can be employed.

As a first step toward adopting cloud computing in the Navy, there is a need to develop a command structure similar to the U.S. DISA that can act as a sponsor and cloud broker on behalf of the Pakistan Navy. Further, this will also help in monitoring the cloud services and ensuring that cybersecurity measures are in place for the protection of data from getting compromised. Finally, before the launch of cloud services for the Pakistan Navy, there is a need to develop a strong IT infrastructure, human resources for management and operation of new technology, and data centers ashore and data nodes on afloat assets.

Developing a culture that will help transform the traditional way of sharing information and resources to a modern way of accessing information remotely via the Internet is very important. Culture for use of the Internet for exchange of information will grow rapidly if the consumers trust the technology and there are no major interruptions or

delays. Thus, the Pakistan Navy may begin with cloud computing by adopting this technology initially at a small scale and as the system is matured, extend it to all of the Navy.

B. RECOMMENDATIONS

Major recommendations of the thesis are summarized here.

- The Pakistan Navy must develop a command structure to support adoption of cloud computing. This command structure must consist of individuals who specialize in IT, cyber operations, and maritime warfare.
- The Pakistan Navy must develop sufficient human resources in IT, systems technology, information warfare, and cyber operations. These personnel will act as a pillar to operate, maintain, and troubleshoot cloud infrastructure for the Navy.
- In order to protect classified data from compromise while using a commercial/international firm's satellite, the Pakistan Navy, in coordination with other arms of the country and the support of the government, must endeavor for the development of a satellite for military communications. The satellite must have sufficient bandwidth to support the requirements of all the armed forces of the country.
- The Pakistan Navy must develop a robust and secure communication infrastructure within the country interconnecting all vital units, bases, and ports for exchange of information up through the TOP SECRET classification level. This infrastructure must be strong enough to withstand the severity of natural calamities and be protected and safe from any act of sabotage. Data rates for exchange of information must be sufficiently high to facilitate smooth streaming and avoid any delays.
- Command structure for implementing cloud computing in coordination with all stakeholders must scrutinize all data to ascertain the correct classification of information and to avoid any inadvertent placement of classified data in servers earmarked for unclassified data.
- Adopting cloud computing in the Navy will be a pilot project among all the armed forces of the country. Considering its importance, future prospects of development and implementation of this technology in true letter and spirit, the Pakistan Navy should endeavor to enhance its annual military budget from the government of the Pakistan. Besides meeting other important requirements, this will provide flexibility to the Navy to acquire the latest hardware and software tools to meet the requirements of the service and to protect the information from eavesdropping.

C. PROSPECTS FOR FUTURE RESEARCH

This thesis has recommended a roadmap for adopting cloud computing within the Pakistan Navy based on unclassified sources. No classified literature could be reviewed, including any that might pertain to the working of cloud computing within classified military environments in any of the countries already using this technology. Moreover, the thesis focused on the current framework for the U.S. Navy's (and the DOD's more generally) use of the cloud. The U.S. Navy's Office of Navy Research is pursuing development of a Navy tactical cloud that will provide warfighters with information necessary for decision making in tactical situations (Brewin, 2014). Tools like data analytics and big data analysis will be the hallmark of the U.S. Navy tactical cloud. Upon development and successful implementation of the U.S. Navy tactical cloud, it could be reviewed for its efficacy and future prospects for the Pakistan Navy.

Since adoption of cloud computing in the Pakistan Navy is a big shift in the methodology of sharing information among all the tiers, there is a need to carefully administer this transition. Besides developing a data center ashore, data nodes on board each ship, aircraft, and submarine will need to be developed. Thus, hardware of various type such as cloud servers, routers, and software interfaces will be required. There is a need to develop a research laboratory for scrutinizing all hardware and software for this project and to explore any hidden backdoors in them. Moreover, if the Pakistan Navy uses commercial cloud vendors for unclassified information, the hardware and software of the commercial vendors may also be verified by the research laboratory.

To become a successful and invincible armed force of a country, sharing of information at all tiers is paramount to support joint operations and achieve desired synergetic efforts for successful accomplishment of the mission. Thus, in order to enhance the mutual exchange of information among all the military services of the Pakistan (i.e., the Pakistan Army, the Pakistan Navy, and the Pakistan Air Force), there is a need to develop a cloud model that can be used by all the services for rapid, secure, and reliable exchange of information. This thesis offers a first step toward such a model, but additional research is needed to extend the model proposed here for the Navy to one that is equally suitable for interservices coordination and exchange of information at all tiers.

Brief overview of addressing connectivity issues pertaining to CENTRIXS are discussed in Appendix B and more research can be done to resolve the connectivity problem.

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A. WORLDWIDE INTEROPERABILITY FOR MICROWAVE ACCESS

Collaboration between ships at sea is important to the completion of a mission. An enormous amount of data is exchanged between these ships. While they are operating in close proximity and in the line-of-sight (LOS), UHF or HF means of communication can be used for mutual exchange of information. However, data exchange rates using UHF/HF are low and may not fulfill the requirements for exchanging large data files or video feeds. The use of a cloud by the Pakistan Navy's ships and other afloat units will require communication with other units and cloud servers over land using satellite.

Traditionally, ships beyond the LOS rely on satellite communications (SATCOM) to exchange vital information. Since the Pakistan Navy does not own a military communication satellite, a commercial satellite will be used. In this case, if each unit communicated with another unit using satellite means, it would saturate the bandwidth of the satellite, and due to limited channel capacity, essential information might not pass through. Additionally, it would likely result in spending a significant portion of the budget as a usage fee for satellite bandwidth. Thus, finding an alternate means for the exchange of information between ships at sea is very important. WiMAX (Worldwide Interoperability for Microwave Access) is one of the best substitutes for exchanging this information in the modern world. Details, as well the benefits, of using WiMAX for exchange of the information are provided below.

Possibly the best method for transferring data between each ship in an afloat cloud infrastructure is via WiMAX (Gillette, 2012). WiMAX is a Fourth Generation (4G) mobile communication standard that is capable of providing ultra-broadband Internet access over wireless communication channels with speeds as high as 70 Mbps (Brian and Grabianowski, n.d.). The biggest advantage of using WiMAX is its range, which allows for sharing information at a distance of up to 30 miles. To exchange data between afloat units, WiMAX antennas or towers could be installed onboard ships. One tower could provide coverage to units spread as far as 3,000 square miles (Brian & Grabianowski, n.d.).

Figure A-1 WiMAX Tower (from Brian and Grabianowski, n.d.)

Practically, WiMAX operates similar to WiFi and offers flexibility to all units to exchange an array of data including email and video without consuming satellite bandwidth. Furthermore, WiMAX's range can be increased if its transmitters are installed on unmanned aerial vehicle (UAV) or air platforms. In case data has to be shared or retrieved from shore authorities, SATCOM can be used by one ship acting as an information coordinator on behalf of other ships in the company. Thus, as shown in Figure A-2 below, among the five ships in formation, the central ship of the formation is acting as a master node of the cloud. A ship designated as a master node of the cloud is responsible for exchange of information with other ships in formation over WiMAX and uses SATCOM for exchange of information with shore authorities. Hence, each ship that remains within the maximum range of WiMAX is communicating with the master node ship, which in turns accesses the cloud server using SATCOM. The U.S. Navy is also in the process of planning and installing an advanced broadband 4G Long-Term Evolution cellular system on ships to allow for the exchange of information using WiMAX (Brewin, 2012). This system will support the exchange of a variety of broadband data between underway ships, freeing them from the constraints of satellite bandwidth (Brewin, 2012).

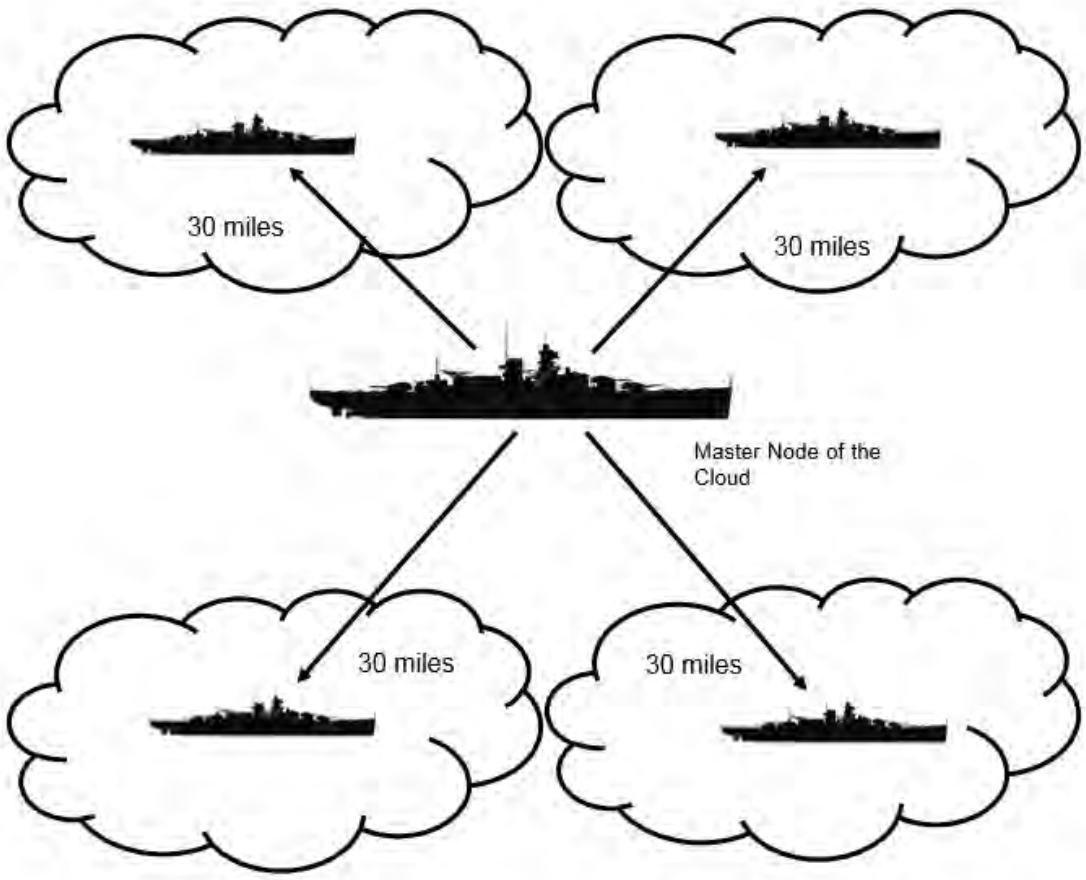


Figure A-2 WiMAX Supported Cloud in Formation

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX B. DEVELOPING CMF CLOUD

The Combined Enterprise Regional Information Exchange System (CENTRIXS) is a standing, global enterprise network allowing U.S. and coalition nations and their forces to securely share operational and intelligence information in support of joint planning, harmony of effort, and decision making in multinational operations (Cook, Lancaster, & Patto, 2007). The CENTRIXS was designed as a hardware and software tool to meet the immediate operational needs of the U.S. Combatant Commands (COCOM) and providing them a platform to share information with coalition partners in the Global War on Terrorism and other rapidly developing military exigencies. DISA defines CENTRIXS as "a system designed to be a global, interoperable, interconnected, inexpensive, and easy-to-use system to share and exchange intelligence and operations information through reliable communications connectivity, data manipulation, and automated processes" (Defense Information Systems Agency [DISA], n.d.). At present there are more than 40 networks associated with CENTRIXS having participants from more than 80 countries (DISA, n.d.). Some of the major networks of CENTRIXS as defined by DISA are as follows:

- CENTRIXS Four Eyes (CFE) for the United States, Britain, Canada, and Australia
- CENTRIXS-J for the United States and Japan
- CENTRIXS-K for the United States and South Korea
- CENTRIXS-ISAF for the International Security Assistance Force (ISAF) in Afghanistan
- CENTRIXS-GCTF for the Troop Contributing Nations of the Global Counter-Terrorism Force (GCTF)
- CENTRIXS-CMFC for the Combined Maritime Forces, Central Command (CMFC)
- CENTRIXS-CMFP for the Combined Maritime Forces, Pacific (CMFP) (DISA, n.d.)

Among the various goals of CENTRIXS, top priority is its immediate availability to its users and COCOM for secure and rapid exchange of information with coalition partners. Although various upgrades in the CENTRIXS have been done over a period of time, concerns with its round-the-clock connectivity and accessibility to coalition

partners is becoming an Achilles heel. Various incidents have occurred in the past where coalition partners could not exchange vital information with the COCOM and other coalition partners involved in the operation due to no connectivity or poor connectivity with CENTRIXS nodes ashore and afloat. Various attempts have been made to improve connectivity problems associated with CENTRIXS. All the hardware and software associated with CENTRIXS are provided by the U.S. DOD suppliers to the U.S. military as well as coalition partners. Thus, the technical solution to the CENTRIXS connectivity issues with the coalition partners is also to be addressed by the U.S. DOD suppliers.

The U.S. DOD and its various arms of defense forces are in the process of adopting cloud computing. The aim behind this shift is to provide warfighters and military commanders with a technology that can enable rapid exchange of information; give an accurate, precise, and error-free picture of battlefield; and help solve various tactical problems. The cloud will allow information resources to be accessed from anywhere around the globe and to be exchanged with any user around the globe having access to the Internet.

In order to resolve the concerns related to connectivity and other technical problems with CENTRIXS, it is proposed that a Combined Maritime Forces (CMF) cloud be developed for coalition partners operating under the CENTCOM. Developing a CMF cloud will provide the following benefits to the U.S. DOD and its users:

- No further requirement of providing CENTRIXS hardware and software tools to coalition partners.
- CMF cloud can be hosted on CENTCOM web servers.
- All data related to CMF mission and task force requirements can be made available to coalition partners via the CMF cloud.
- Applications for chat and video conferencing can be provided for rapid exchange of information during conduct of a mission.
- Coalition partners having specific root certificates, CAC card access, and VPN installed on their computers will be authorized to join the CMF cloud and chat rooms.
- Establishing CMF cloud will allow the coalition partners to utilize their own hardware and Internet connectivity to access an enormous pool of information available at CMF web servers. Furthermore, connectivity problems associated with CENTRIXS will no longer become a hurdle in the conduct of a mission and rapid exchange of vital information.

LIST OF REFERENCES

30m Internet users in Pakistan. (2013, June 24). *The Express Tribune.* Retrieved from http://tribune.com.pk/story/567649/30m-internet-users-in-pakistan-half-on-mobile-report/

Ansari, A. (2012). The journey of IT in Pakistan. *UTrade eMagazine*. Retrieved from http://www.utrade.co/Magazine/Utrade-Magazine.aspx?Key=409&Title=The+Journey+of+IT+in+Pakistan

Antonopoulos, N., & Gillam, L. (2010). *Cloud computing principles, systems and applications*. New York, NY: Springer.

Armbrust, M., Fox, A., Griffith, R., Joseph, A. D., Katz, R., Konwinski, A., & Zaharia, M. (2010). A view of cloud computing. *Communications of the ACM, 53*(4), 50–58.

Asia Cloud Computing Association. (2014). *Cloud research index*. Retrieved from http://asiacloudcomputing.org/research/cri2014

Barroso, L. A., & Hölzle, U. (2009). *The datacenter as a computer: An introduction to the design of warehouse-scale machines*. San Rafael, CA: Morgan and Claypool.

Brewin, B. (2012). Naval Air Systems Command plans 4G cell service aboard ships. Retrieved from http://www.nextgov.com/mobile/2012/04/naval-air-systems-command-plans-4g-cell-service-aboard-ships/51015/

Brewin, B. (2014). The Navy wants a tactical cloud. Retrieved from http://www.defenseone.com/technology/2014/09/navy-wants-tactical-cloud/95129/

Brian, M., & Grabianowski, E. (n.d.). How WiMAX works. Retrieved from http://computer.howstuffworks.com/wimax2.htm

Buyya, R., Yeo, C. S., Venugopal, S., Broberg, J., & Brandic, I. (2009). Cloud computing and emerging IT platforms: Vision, hype, and reality for delivering computing as the fifth utility. *Future Generation Computer Systems*, *25*(6), 599–616.

Corrin, A. (2014). Navy targets cloud for command and control, email capabilities. *C4ISR & Networks.* Retrieved from http://www.c4isrnet.com/article/20140926/C4ISRNET14/309260004/Nay-targets-cloud-command-control-email-capabilities

Cook, A. D., Lancaster, P. E., & Patto, R. R. (2007). *The Combined Enterprise Regional Information Exchange System—The way ahead* (Master's thesis). Naval Postgraduate School, Monterey, CA.

Cube XS Weatherly Cloud Services (CWCS). (n.d.). Retrieved from https://www.cubexsweatherly.com/home.html

Curtis, D. (2012). Steve Jobs and the cloud. Retrieved from http://dcurt.is/steve-jobs-and-the-cloud

Department of Defense Chief Information Officer. (2012). *Cloud computing strategy*. Washington, DC: Author.

Department of Navy Chief Information Officer. (2013, July 31). *Enterprise mobility and cloud service pilot project governance* (Memorandum). Washington, DC: Author.

Defense Information Systems Agency. (n.d.). Multinational information sharing (MNIS). Retrieved from http://www.disa.mil/Mission-Support/Command-and-Control/MNIS

Geczy, P., Izumi, N., & Hasida, K. (2012). Cloudsourcing: Managing cloud adoption. *Global Journal of Business Research*, *6*(2), 57–70.

Gillette, S. E. (2012). *Cloud computing and virtual desktop infrastructures in afloat environments* (Master's thesis). Naval Postgraduate School, Monterey, CA.

Gupta, S., Kumar, P., & Abraham, A. (2013). A profile based network intrusion detection and prevention system for securing cloud environment. *International Journal of Distributed Sensor Networks*, 1–12.

Hess, K. (2011). 10 advantages of SAN vs. DAN. Retrieved from http://www.serverwatch.com/trends/article.php/3925351/10-Advantages-of-SAN-vs-DAS.htm

Hofmann, P., & Woods, D. (2010). Cloud computing: The limits of public clouds for business applications. *IEEE Internet Computing, 14*(6), 90–95.

Krutz, R. L., & Vines, R. D. (2010). *Cloud security: A comprehensive guide to secure cloud computing*. Hoboken, NJ: Wiley.

Market Research. (2014). Global cloud computing market forecast 2015–2020. Retrieved from http://www.marketresearchmedia.com/?p=839

National Institute of Standards and Technology. (2011a). *NIST cloud computing reference architecture* (SP 500-292). Gaithersburg, MD: Author.

National Institute of Standards and Technology. (2011b). *The NIST definition of cloud computing* (SP 800-145). Gaithersburg, MD: Author.

National Institute of Standards and Technology. (2011c). *U.S. government cloud computing technology roadmap, volume I, release 1.0 (draft): High-priority*

requirements to further USG agency cloud computing adoption (SP 500-293). Gaithersburg, MD: Author.

Orakwue, E. (2010). Private clouds: Secure managed services. *Information Security Journal*, *19*(6), 295–298.

Pakistan Software Board. (n.d.). Retrieved from http://www.pseb.org.pk/why-pakistan.html

Pakistan Software Export Board. (2014). Industry overview. Retrieved from http://www.pseb.org.pk/industry-overview.html

Pakistan Telecommunication Limited. (2014). Retrieved from http://ptclcloud.com.pk/

Plummer, D. C., Smith, D. M., Bittman, T. J., Cearley, D. W., Cappuccio, D. J., Scott, D., Kumar, R., & Robertson, B. (2009). *Five refining attributes of public and private cloud computing* (Gartner Research Report). Stamford, CT: Gartner.

Rapid Compute. (2014). Retrieved from https://www.rapidcompute.com/

Rimal, B. P., Choi, E., & Lumb, I. (2010). A taxonomy, survey, and issues of cloud computing ecosystem. In N. Antonopolous & L. Gillam (eds.) *Cloud Computing: Principles, Systems and Applications* (pp. 21–46). London: Springer-Verlag.

Scholz, J. A. (2013). *Enterprise architecture and information assurance—Developing a secure foundation.* Boca Raton, FL: Auerbach Publications.

Sotomayor, B., Montero, R. S., Llorente, I. M., & Foster, I. (2009). Virtual infrastructure management in private and hybrid clouds. *IEEE Internet Computing*, *13*(5), 14–23.

Thampi, S. M., Bhargava, B., & Atrey, P. K. (2013). *Managing trust in cyberspace.* London, England: Chapman and Hall.

Verge, J. (2014, March 14). U.S. Navy shifting public data to Amazon Cloud. Retrieved from http://www.datacenterknowledge.com/archives/2014/03/14/u-s-navy-shifting-public-data-amazon-cloud/

WebDweb Web Systems. (n.d.). SAAS services. Retrieved from http://www.webdweb.com/services/saas-services/

Winkler, V. (2011). *Securing the cloud—Cloud computer security techniques and tactics*. Rockland, MA: Syngress.

Zhou, H. (2012). *The internet of things in the cloud—A middleware perspective.* Boca Raton, FL: CRC Press.

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California